

Advanced Scan | S-DC | Full Port

Report generated by Tenable Nessus™ Thu, 08 Jan 2026 17:42:50 EST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.1.1 4

Vulnerabilities by Host

192.168.1.1



Scan Information

Start time:	Thu Jan 8 16:48:50 2026
End time:	Thu Jan 8 17:42:49 2026

Host Information

DNS Name:	S-DC.swansea.acca
Netbios Name:	S-DC
IP:	192.168.1.1
MAC Address:	08:00:27:2A:B5:B6 08:00:27:1A:80:9D 08:00:27:99:DA:4A
OS:	Microsoft Windows Server 2022 Datacenter Build 20348

Vulnerabilities

261807 - KB5065432: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (September 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5065432 or hotpatch 5065306. It is, therefore, affected by multiple vulnerabilities

- SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks: SMB Server signing SMB Server Extended Protection for Authentication (EPA) Microsoft is releasing this CVE to provide customers with audit capabilities to help them to assess their environment and to identify any potential device or software incompatibility issues before deploying SMB Server hardening measures that protect against relay attacks. If you have not already enabled SMB Server hardening measures, we advise customers to take the following actions to be protected from these relay attacks:

Assess your environment by utilizing the audit capabilities that we are exposing in the September 2025 security updates. See Support for Audit Events to deploy SMB Server HardeningSMB Server Signing & SMB Server EPA. Adopt appropriate SMB Server hardening measures. (CVE-2025-55234)

- Improper restriction of communication channel to intended endpoints in Windows PowerShell allows an authorized attacker to elevate privileges locally. (CVE-2025-49734)

- Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network. (CVE-2025-53796, CVE-2025-53797, CVE-2025-53798, CVE-2025-53806)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://support.microsoft.com/help/5065432

https://support.microsoft.com/help/5065306

Solution

Apply Security Update 5065432 or hotpatch 5065306

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2025-49734
CVE	CVE-2025-53796
CVE	CVE-2025-53797
CVE	CVE-2025-53798

CVE	CVE-2025-53799
CVE	CVE-2025-53800
CVE	CVE-2025-53801
CVE	CVE-2025-53802
CVE	CVE-2025-53803
CVE	CVE-2025-53804
CVE	CVE-2025-53805
CVE	CVE-2025-53806
CVE	CVE-2025-53807
CVE	CVE-2025-53808
CVE	CVE-2025-53810
CVE	CVE-2025-54091
CVE	CVE-2025-54092
CVE	CVE-2025-54093
CVE	CVE-2025-54094
CVE	CVE-2025-54095
CVE	CVE-2025-54096
CVE	CVE-2025-54097
CVE	CVE-2025-54098
CVE	CVE-2025-54099
CVE	CVE-2025-54101
CVE	CVE-2025-54102
CVE	CVE-2025-54104
CVE	CVE-2025-54106
CVE	CVE-2025-54107
CVE	CVE-2025-54109
CVE	CVE-2025-54110
CVE	CVE-2025-54111
CVE	CVE-2025-54112
CVE	CVE-2025-54113
CVE	CVE-2025-54114
CVE	CVE-2025-54115
CVE	CVE-2025-54116
CVE	CVE-2025-54894
CVE	CVE-2025-54895
CVE	CVE-2025-54911
CVE	CVE-2025-54912
CVE	CVE-2025-54913
CVE	CVE-2025-54915
CVE	CVE-2025-54916
CVE	CVE-2025-54917
CVE	CVE-2025-54918
CVE	CVE-2025-54919

CVE	CVE-2025-55223
CVE	CVE-2025-55224
CVE	CVE-2025-55225
CVE	CVE-2025-55226
CVE	CVE-2025-55228
CVE	CVE-2025-55234
CVE	CVE-2025-55236
CVE	CVE-2025-59220
MSKB	5065432
MSKB	5065306
XREF	MSFT:MS25-5065432
XREF	MSFT:MS25-5065306
XREF	IAVA:2025-A-0670-S
XREF	IAVA:2025-A-0671-S
XREF	CWE:41
XREF	CWE:121
XREF	CWE:122
XREF	CWE:125
XREF	CWE:126
XREF	CWE:190
XREF	CWE:200
XREF	CWE:209
XREF	CWE:284
XREF	CWE:287
XREF	CWE:362
XREF	CWE:367
XREF	CWE:416
XREF	CWE:693
XREF	CWE:822
XREF	CWE:843
XREF	CWE:908
XREF	CWE:923

Plugin Information

Published: 2025/09/09, Modified: 2025/10/29

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5065432
  - 5065306
```

```
  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.20348.4050
    Should be      : 10.0.20348.4163
```

274789 - KB5068787: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (November 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5068787. It is, therefore, affected by multiple vulnerabilities

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2025-60724, CVE-2025-60714, CVE-2025-60715, CVE-2025-62452)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information.

(CVE-2025-59509, CVE-2025-59513, CVE-2025-60706, CVE-2025-62208, CVE-2025-62209)

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.

(CVE-2025-59505, CVE-2025-59506, CVE-2025-59507, CVE-2025-59508, CVE-2025-59511, CVE-2025-59512, CVE-2025-59514, CVE-2025-59515, CVE-2025-60703, CVE-2025-60704, CVE-2025-60705, CVE-2025-60707, CVE-2025-60709, CVE-2025-60713, CVE-2025-60716, CVE-2025-60717, CVE-2025-60719, CVE-2025-60720, CVE-2025-62213, CVE-2025-62215, CVE-2025-62217)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://support.microsoft.com/help/5068787

Solution

Apply Security Update 5068787

Risk Factor

Critical

CVSS v3.0 Base Score

7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2025-59505
CVE	CVE-2025-59506
CVE	CVE-2025-59507
CVE	CVE-2025-59508
CVE	CVE-2025-59509
CVE	CVE-2025-59510
CVE	CVE-2025-59511
CVE	CVE-2025-59512
CVE	CVE-2025-59513
CVE	CVE-2025-59514
CVE	CVE-2025-60703
CVE	CVE-2025-60704
CVE	CVE-2025-60705
CVE	CVE-2025-60706
CVE	CVE-2025-60707
CVE	CVE-2025-60708
CVE	CVE-2025-60709
CVE	CVE-2025-60713
CVE	CVE-2025-60714
CVE	CVE-2025-60715
CVE	CVE-2025-60716
CVE	CVE-2025-60719
CVE	CVE-2025-60720
CVE	CVE-2025-60723
CVE	CVE-2025-60724
CVE	CVE-2025-62213
CVE	CVE-2025-62215
CVE	CVE-2025-62217
CVE	CVE-2025-62452
MSKB	5068787
XREF	MSFT:MS25-5068787
XREF	CISA-KNOWN-EXPLOITED:2025/12/03
XREF	IAVA:2025-A-0850
XREF	IAVA:2025-A-0851

Plugin Information

Published: 2025/11/11, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5068787

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.20348.4050
    Should be      : 10.0.20348.4405
```

270390 - KB5066782: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (October 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5066782. It is, therefore, affected by multiple vulnerabilities

- tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka Predictor heap-buffer-overflow. (CVE-2016-9535)

- In IGEL OS before 11, Secure Boot can be bypassed because the igel-flash-driver module improperly verifies a cryptographic signature. Ultimately, a crafted root filesystem can be mounted from an unverified SquashFS image. (CVE-2025-47827)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://support.microsoft.com/help/5066782

Solution

Apply Security Update 5066782

Risk Factor

High

CVSS v3.0 Base Score

9.9 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2016-9535
CVE	CVE-2025-24052
CVE	CVE-2025-24990
CVE	CVE-2025-25004
CVE	CVE-2025-47827
CVE	CVE-2025-48813
CVE	CVE-2025-49708
CVE	CVE-2025-50152
CVE	CVE-2025-50175
CVE	CVE-2025-54957
CVE	CVE-2025-55325
CVE	CVE-2025-55326
CVE	CVE-2025-55328
CVE	CVE-2025-55331
CVE	CVE-2025-55332
CVE	CVE-2025-55333
CVE	CVE-2025-55335
CVE	CVE-2025-55336
CVE	CVE-2025-55338
CVE	CVE-2025-55339
CVE	CVE-2025-55340
CVE	CVE-2025-55678
CVE	CVE-2025-55679
CVE	CVE-2025-55680
CVE	CVE-2025-55681
CVE	CVE-2025-55683
CVE	CVE-2025-55685
CVE	CVE-2025-55686
CVE	CVE-2025-55687
CVE	CVE-2025-55689
CVE	CVE-2025-55692
CVE	CVE-2025-55695
CVE	CVE-2025-55696
CVE	CVE-2025-55699
CVE	CVE-2025-55700
CVE	CVE-2025-55701
CVE	CVE-2025-58714
CVE	CVE-2025-58715

CVE	CVE-2025-58716
CVE	CVE-2025-58717
CVE	CVE-2025-58718
CVE	CVE-2025-58719
CVE	CVE-2025-58720
CVE	CVE-2025-58722
CVE	CVE-2025-58725
CVE	CVE-2025-58726
CVE	CVE-2025-58729
CVE	CVE-2025-58730
CVE	CVE-2025-58731
CVE	CVE-2025-58732
CVE	CVE-2025-58733
CVE	CVE-2025-58734
CVE	CVE-2025-58735
CVE	CVE-2025-58736
CVE	CVE-2025-58737
CVE	CVE-2025-58738
CVE	CVE-2025-58739
CVE	CVE-2025-59184
CVE	CVE-2025-59185
CVE	CVE-2025-59186
CVE	CVE-2025-59187
CVE	CVE-2025-59188
CVE	CVE-2025-59190
CVE	CVE-2025-59191
CVE	CVE-2025-59192
CVE	CVE-2025-59193
CVE	CVE-2025-59195
CVE	CVE-2025-59196
CVE	CVE-2025-59197
CVE	CVE-2025-59198
CVE	CVE-2025-59199
CVE	CVE-2025-59200
CVE	CVE-2025-59201
CVE	CVE-2025-59202
CVE	CVE-2025-59203
CVE	CVE-2025-59204
CVE	CVE-2025-59205
CVE	CVE-2025-59207
CVE	CVE-2025-59208
CVE	CVE-2025-59209
CVE	CVE-2025-59211

CVE	CVE-2025-59214
CVE	CVE-2025-59230
CVE	CVE-2025-59242
CVE	CVE-2025-59244
CVE	CVE-2025-59253
CVE	CVE-2025-59254
CVE	CVE-2025-59255
CVE	CVE-2025-59258
CVE	CVE-2025-59259
CVE	CVE-2025-59260
CVE	CVE-2025-59261
CVE	CVE-2025-59275
CVE	CVE-2025-59277
CVE	CVE-2025-59278
CVE	CVE-2025-59280
CVE	CVE-2025-59282
CVE	CVE-2025-59294
CVE	CVE-2025-59295
MSKB	5066782
XREF	MSFT:MS25-5066782
XREF	CISA-KNOWN-EXPLOITED:2025/11/04
XREF	IAVA:2025-A-0775-S
XREF	IAVA:2025-A-0776-S

Plugin Information

Published: 2025/10/14, Modified: 2025/11/18

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5066782

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.20348.4050
    Should be      : 10.0.20348.4294
```

10412 - Microsoft Windows SMB Registry : Autologon Enabled

Synopsis

Anyone can logon to the remote system.

Description

This script determines whether the autologon feature is enabled. This feature allows an intruder to log into the remote host as DefaultUserName with the password DefaultPassword.

See Also

http://support.microsoft.com/kb/315231

Solution

Delete the keys AutoAdminLogon and DefaultPassword under HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

References

MSKB	324737

Plugin Information

Published: 2000/05/20, Modified: 2022/08/16

Plugin Output

tcp/445/cifs

```
Autologon is enabled on this host.
This allows an attacker to access the domain: SWANSEA as testuser@swansea.acca/w******s

Note: The password displayed has been partially obfuscated.
```

166555 - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Synopsis

The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config \EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

http://www.nessus.org/u?9780b9d2

Solution

Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config \EnableCertPaddingCheck

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.6 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2013-3900
XREF	CISA-KNOWN-EXPLOITED:2022/07/10
XREF	IAVA:2013-A-0227

Plugin Information

Published: 2022/10/26, Modified: 2025/10/22

Plugin Output

tcp/445/cifs

```
Nessus detected the following potentially insecure registry key configuration:
   - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the
registry.
   - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not
present in the registry.
```

10043 - Chargen UDP Service Remote DoS

Synopsis

The remote host is running a 'chargen' service.

Description

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay.

An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

See Also

http://www.nessus.org/u?f0dbdf05

Solution

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-1999-0103

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/11/29, Modified: 2020/06/12

Plugin Output

udp/19

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.

- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

tcp/7/echo

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.

- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

udp/7

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-1999-0511

Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

```
IP forwarding appears to be enabled on the remote host.

 Detected local MAC Address        : 0800271ffc7b
 Response from local MAC Address   : 0800271ffc7b

 Detected Gateway MAC Address      : 0800272ab5b6
 Response from Gateway MAC Address : 0800272ab5b6
```

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

tcp/17/qotd

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE	CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

udp/17/qotd

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=S-DC
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/443/www

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/443/www

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

132101 - Windows Speculative Execution Configuration Check

Synopsis

The remote host has not properly mitigated a series of speculative execution vulnerabilities.

Description

The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by :

- Branch Target Injection (BTI) (CVE-2017-5715)
- Bounds Check Bypass (BCB) (CVE-2017-5753)
- Rogue Data Cache Load (RDCL) (CVE-2017-5754)
- Rogue System Register Read (RSRE) (CVE-2018-3640)
- Speculative Store Bypass (SSB) (CVE-2018-3639)
- L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)
- Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)
- Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)
- Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)
- Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)
- TSX Asynchronous Abort (TAA) (CVE-2019-11135)
- Intel Branch History Injection (BHI) (CVE-2022-0001)

See Also

http://www.nessus.org/u?8902cebb

http://www.nessus.org/u?6a005ed4

Solution

Apply vendor recommended settings.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.2 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

5.4 (CVSS2#AV:L/AC:M/Au:N/C:C/I:P/A:N)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	102371
BID	102378
BID	104232
BID	105080
BID	108330
CVE	CVE-2017-5715
CVE	CVE-2017-5753
CVE	CVE-2017-5754
CVE	CVE-2018-3615
CVE	CVE-2018-3620
CVE	CVE-2018-3639
CVE	CVE-2018-3646
CVE	CVE-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2019-11135
CVE	CVE-2022-0001
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Exploitable With

CANVAS (true)

Plugin Information

Published: 2019/12/18, Modified: 2025/08/27

Plugin Output

tcp/445/cifs

```
Current Settings:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: Not Set
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: Not Set
```

```
-----------------------------------

Recommended Settings:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: 0x00000003 (3)
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: 0x00000048 (72)
  CVEs Covered:
    CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-3615, CVE-2018-3620,
    CVE-2018-3639, CVE-2018-3646, CVE-2018-11091, CVE-2018-12126, CVE-2018-12127,
    CVE-2018-12130, CVE-2019-11135
  Note: Full mitigation for CVE-2018-3639 (Speculative Store Bypass).
```

10663 - DHCP Server Detection

Synopsis

The remote DHCP server may expose information about the associated network.

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Risk Factor

Low

CVSS v2.0 Base Score

3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2001/05/05, Modified: 2019/03/06

Plugin Output

udp/67

```
Nessus gathered the following information from the remote DHCP server :

  Master DHCP server of this network : 192.168.1.1
  IP address the DHCP server would attribute us : 192.168.1.50
  Netmask : 255.255.255.0
  DHCP server(s) identifier : 192.168.1.1
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is 1 second.
```

16193 - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?3ed73b52

https://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/01/18, Modified: 2025/05/27

Plugin Output

tcp/445/cifs

```
Forefront_Endpoint_Protection :

A Microsoft anti-malware product is installed on the remote host :

  Product name                 : Windows Defender
  Path                         : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25110.6-0\
  Version                      : 4.18.25110.6
  Engine version               : 1.1.25110.1
  Antivirus signature version  : 1.443.564.0
  Antispyware signature version : 1.443.564.0
```

92415 - Application Compatibility Cache

Synopsis

Nessus was able to gather application compatibility settings on the remote host.

Description

Nessus was able to generate a report on the application compatibility cache on the remote Windows host.

See Also

https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

http://www.nessus.org/u?4a076105

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/23

Plugin Output

tcp/0

```
Application compatibility cache report attached.
```

34097 - BIOS Info (SMB)

Synopsis

BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's SMB interface.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/06/11

Plugin Output

tcp/0

```
Version      : VirtualBox
Release date : 20061201000000.000000+000
Secure boot  : disabled
```

34096 - BIOS Info (WMI)

Synopsis

The BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's WMI interface.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/05, Modified: 2025/12/08

Plugin Output

tcp/0

```
Vendor       : innotek GmbH
Version      : VirtualBox
Release date : 20061201000000.000000+000
UUID         : DFF36028-F2DF-4C42-A41B-ED49D57E2617
Secure boot  : disabled
```

10761 - COM+ Internet Services (CIS) Server Detection

Synopsis

A COM+ Internet Services (CIS) server is listening on this port.

Description

COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

See Also

http://www.nessus.org/u?d02f7e6e

https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp

Solution

If you do not use this service, disable it with DCOMCNFG.

Otherwise, limit access to this port.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/3388/ncacn_http

```
Server banner :

ncacn_http/1.0
```

10761 - COM+ Internet Services (CIS) Server Detection

Synopsis

A COM+ Internet Services (CIS) server is listening on this port.

Description

COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall.

See Also

http://www.nessus.org/u?d02f7e6e

https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp

Solution

If you do not use this service, disable it with DCOMCNFG.

Otherwise, limit access to this port.

Risk Factor

None

Plugin Information

Published: 2001/09/14, Modified: 2019/11/22

Plugin Output

tcp/64492/ncacn_http

```
Server banner :

ncacn_http/1.0
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/09/29

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_server_2022:10.0.20348.4052:-:~~datacenter~~x64~ -> Microsoft Windows
 Server 2022

Following application CPE's matched on the remote system :

  cpe:/a:haxx:curl:8.13.0.0 -> Haxx Curl
  cpe:/a:microsoft:.net_framework:4.8 -> Microsoft .NET Framework
  cpe:/a:microsoft:.net_framework:4.8.4775.0 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:143.0.3650.96 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.1.20348.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:iis:10.0 -> Microsoft IIS
  cpe:/a:microsoft:internet_explorer:11.0.20348.4050 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_information_services:10.0.20348.2849 -> Microsoft Internet Information
 Server (IIS) -
  cpe:/a:microsoft:remote_desktop_connection:10.0.20348.2849 -> Microsoft Remote Desktop Connection
  cpe:/a:microsoft:sql_server:12.0.5214.6 -> Microsoft SQLServer
```

```
 cpe:/a:microsoft:system_center_endpoint_protection:4.18.25110.6 -> Microsoft System Center
Endpoint Protection
 cpe:/a:microsoft:windows_defender:4.18.25110.6 -> Microsoft Windows Defender
 cpe:/a:tenable:nessus -> Tenable Nessus
 cpe:/a:tenable:nessus:10.10.0 -> Tenable Nessus
 x-cpe:/a:microsoft:dhcp_server:10.0.20348.3932
```

24270 - Computer Manufacturer Information (WMI)

Synopsis

It is possible to obtain the name of the remote computer manufacturer.

Description

By making certain WMI queries, it is possible to obtain the model of the remote computer as well as the name of its manufacturer and its serial number.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/02, Modified: 2025/12/08

Plugin Output

tcp/0

```
Computer Manufacturer : innotek GmbH
Computer Model : VirtualBox
Computer SerialNumber : VirtualBox-dff36028-f2df-4c42-a41b-ed49d57e2617
Computer Type : Other

Computer Physical CPU's : 1
Computer Logical CPU's  : 2
  CPU0
    Architecture  : x64
    Physical Cores: 2
    Logical Cores : 2

Computer Memory : 4095 MB
```

171860 - Curl Installed (Windows)

Synopsis

Curl is installed on the remote Windows host.

Description

Curl, a command line tool for transferring data with URLs, was detected on the remote Windows host.

Please note, if the installation is located in either the Windows\System32 or Windows\SysWOW64 directory, it will be considered as managed by the OS. In this case, paranoid scanning is require to trigger downstream vulnerabilty checks. Paranoid scanning has no affect on this plugin itself.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/23, Modified: 2025/12/08

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path          : c:\windows\system32\curl.exe
  Version       : 8.13.0.0
  Managed by OS : True

  Path          : c:\windows\syswow64\curl.exe
  Version       : 8.13.0.0
  Managed by OS : True
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : NETLOGON_LRPC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : OLE0BF8E51F21A26D387856B566CF81

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : NTDS_LPC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
```

```
Named pipe : MicrosoftLaps_LRPC_0fb2f016-fe45-4a08-a7f9-a467f5e5fa0b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5180FE7693E37C0664DD72F7B63A

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9c61d91b7fc03d8480

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5180FE7693E37C0664DD72F7B63A

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Name [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\7840aefca19f774e
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
```

```
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S-DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Descr [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/5504/dce-rpc

```
The following DCERPC services are available on TCP port 5504 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ed96b012-c8ce-4f60-a682-35535b12ff75, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 5504
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49664/dce-rpc

```
The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 7364746e-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
```

```
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-0000000000 [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49665/dce-rpc

```
The following DCERPC services are available on TCP port 49665 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49666/dce-rpc

```
The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49667/dce-rpc

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49668/dce-rpc

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 7364746e-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/54401/dce-rpc

```
The following DCERPC services are available on TCP port 54401 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 54401
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64493/dce-rpc

```
The following DCERPC services are available on TCP port 64493 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 64493
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64493
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64493
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
```

```
TCP Port : 64493
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64493
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64499/dce-rpc

```
The following DCERPC services are available on TCP port 64499 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6bffd098-a112-3610-9833-46c3f874532d, version 1.0
Description : DHCP Server Service
Windows process : unknown
Type : Remote RPC service
TCP Port : 64499
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5b821720-f63b-11d0-aad2-00c04fc324db, version 1.0
Description : DHCP Server Service
Windows process : unknown
Type : Remote RPC service
TCP Port : 64499
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64501/dce-rpc

```
The following DCERPC services are available on TCP port 64501 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0
Description : DNS Server
Windows process : dns.exe
Type : Remote RPC service
TCP Port : 64501
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64509/dce-rpc

```
The following DCERPC services are available on TCP port 64509 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 64509
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 64509
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 64509
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
```

```
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 64509
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64539/dce-rpc

```
The following DCERPC services are available on TCP port 64539 :

Object UUID : 5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c
UUID : 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1.0
Description : Unknown RPC service
Annotation : Frs2 Service
Type : Remote RPC service
TCP Port : 64539
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64558/dce-rpc

```
The following DCERPC services are available on TCP port 64558 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 64558
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64559/dce-rpc

```
The following DCERPC services are available on TCP port 64559 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : aa177641-fc9b-41bd-80ff-f964a701596f, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64559
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c95fc993-f460-4763-a00d-bb3b9e5c7e2e, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64559
IP : 192.168.1.1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 32e36e84-4ba2-496c-ba85-fb450f325107, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64559
IP : 192.168.1.1
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/64639/dce-rpc

```
The following DCERPC services are available on TCP port 64639 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3357951c-a1d1-47db-a278-ab945d063d03, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 64639
IP : 192.168.1.1
```

121509 - DHCP Server Detection (Windows)

Synopsis

A DHCP server is installed on the remote Windows host.

Description

A DHCP server is installed on the remote Windows host.

See Also

http://www.nessus.org/u?5a5ed447

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0938

Plugin Information

Published: 2019/01/31, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Path         : C:\Windows\System32\
Version      : 10.0.20348.3932
File Version : Windows DHCP Server (10.0.20348.3932)
```

139785 - DISM Package List (Windows)

Synopsis

Use DISM to extract package info from the host.

Description

Using the Deployment Image Servicing Management tool, this plugin enumerates installed packages.

See Also

http://www.nessus.org/u?cbb428b2

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/08/25, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
The following packages were enumerated using the Deployment Image Servicing and Management Tool:

Package      : Downlevel-NLS-Sorting-Versions-Server-FoD-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/05/2021 09:38

Package      : Downlevel-NLS-Sorting-Versions-Server-FoD-
Package~31bf3856ad364e35~wow64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/05/2021 09:38

Package      : Microsoft-OneCore-DirectX-Database-FOD-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/05/2021 09:38

Package      : Microsoft-OneCore-RasSstp-Api-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : Feature Pack
Install Time : 24/09/2025 15:57

Package      : Microsoft-Windows-FodMetadata-Package~31bf3856ad364e35~amd64~~10.0.20348.1
```

```
State        : Installed
Release Type : Feature Pack
Install Time : 08/05/2021 09:37

Package      : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : Foundation
Install Time : 08/05/2021 08:24

Package      : Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~11.0.20348.3451
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/08/2025 16:32

Package      : Microsoft-Windows-LanguageFeatures-Basic-en-gb-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 24/09/2025 15:23

Package      : Microsoft-Windows-LanguageFeatures-Basic-en-us-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/05/2021 09:37

Package      : Microsoft-Windows-LanguageFeatures-Handwriting-en-us-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 08/05/2021 09:38

Package      : Microsoft-Windows-LanguageFeatures-OCR-en-gb-Package~31bf3856ad36 [...]
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.

- On Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

tcp/13/daytime

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.

- On Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

udp/13/daytime

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/12/08

Plugin Output

tcp/0

```
Hostname : S-DC
  S-DC (WMI)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

11367 - Discard Service Detection

Synopsis

A discard service is running on the remote host.

Description

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.

This service is unused these days, so it is advised that you disable it.

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information

Published: 2003/03/12, Modified: 2011/03/11

Plugin Output

tcp/9/discard

71246 - Enumerate Local Group Memberships

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.

Description

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.

Note: Unable to query local Domain Controllers during Agent scans.
Rendering Group data obtained by plugin 171956.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/12/06, Modified: 2025/12/08

Plugin Output

tcp/0

```
Group Name : Server Operators
Host Name  : S-DC
Group SID  : S-1-5-32-549
Members    :

Group Name : Account Operators
Host Name  : S-DC
Group SID  : S-1-5-32-548
Members    :

Group Name : Pre-Windows 2000 Compatible Access
Host Name  : S-DC
Group SID  : S-1-5-32-554
Members    :
  Name : Authenticated Users
    Domain : S-DC
    Class  : Win32_SystemAccount
    SID    : S-1-5-11

Group Name : Incoming Forest Trust Builders
Host Name  : S-DC
Group SID  : S-1-5-32-557
Members    :

Group Name : Windows Authorization Access Group
Host Name  : S-DC
Group SID  : S-1-5-32-560
Members    :
```

```
  Name : ENTERPRISE DOMAIN CONTROLLERS
    Domain : S-DC
    Class  : Win32_SystemAccount
    SID    : S-1-5-9

Group Name : Terminal Server License Servers
Host Name  : S-DC
Group SID  : S-1-5-32-561
Members    :

Group Name : Administrators
Host Name  : S-DC
Group SID  : S-1-5-32-544
Members    :
  Name : Administrator
    Domain : SWANSEA
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3861473089-3053040122-1338177554-500
  Name : Enterprise Admins
    Domain : SWANSEA
    Class  : Win32_Group
    SID    : S-1-5-21-3861473089-3053040122-1338177554-519
  Name : Domain Admins
    Domain : SWANSEA
    Class  : Win32_Group
    SID    : S-1-5-21-3861473089-3053040122-1338177554-512

Group Name : Users
Host Name  : S-DC
Group SID  : S-1-5-32-545
Members    :
  Name : INTERACTIVE
    Domain : S-DC
    Class  : Win32_SystemAccount
    SID    : S-1-5-4
  Name : Authenticated Users
    Domain : S-DC
    Class  : Win32_SystemAccount
    SID    : S-1-5-11
  Name : Domain Users
    Domain : SWANSEA
    Class  : Win32_Group
    SID    : S-1-5-21-3861473089-3053040122-1338177554-513

Group Name : Guests
Host Name  : S-DC
Group SID  : S-1-5-32-546
Members    :
  Name : Guest
    Domain : SWANSEA
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3861473089-3053040122-1338177554-501
  Name : Domain Guests
    Domain : SWANSEA
    Class  : Win32_Group
    SID    : S-1-5-21-3861473089-3053040122-1338177554-514

Group Name : Print Ope [...]
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/12/08

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:2A:B5:B6 : PCS Systemtechnik GmbH
08:00:27:1A:80:9D : PCS Systemtechnik GmbH
08:00:27:99:DA:4A : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:2A:B5:B6
  - 08:00:27:1A:80:9D
  - 08:00:27:99:DA:4A
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220-Microsoft FTP Service
220 Welcome to SWANSEA.ACCA Network!!!!
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: NTLM TlRMTVNTUAACAAAADgAOADgAAAAFgokCYw/
V9HpxUT0AAAAAAAAAAIwAjABGAAAACgB8TwAAAA9TAFcAQQBOAFMARQBBAAIADgBTAFcAQQBOAFMARQBBAAEACABTAC0ARABDAAQAGABzAHcAYQBuA
+mA3AEAAAAA
Date: Thu, 08 Jan 2026 21:52:58 GMT
Content-Length: 341

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  GET  HEAD  POST  TRACE OPTIONS are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/5985/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8834/www

```
The remote web server type is :

NessusWWW
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/47001/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

170631 - Host Active Directory Configuration (Windows)

Synopsis

The Windows host is joined to an Active Directory domain.

Description

The Windows host is joined to an Active Directory domain and it was possible to retrieve certain Active Directory configuration attributes, including:

Computer information in AD:

- Common Name
- DNS Name
- Distinguished Name
- Domain Role
- Object SID
- SamAccountName

AD domain and forest information:

- Domain FQDN
- Domain GUID
- Domain NetBIOS Name
- Domain SID
- Forest FQDN

See Also

http://www.nessus.org/u?56077cfb

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/25, Modified: 2025/12/08

Plugin Output

tcp/0

```
Computer information in AD:
  Common Name        : CN=S-DC
  DNS Name           : S-DC
  Distinguished Name : CN=S-DC,OU=Domain Controllers,DC=swansea,DC=acca
  Domain Role        : PrimaryDomainController
  Object SID         : S-1-5-21-3861473089-3053040122-1338177554-1001
  SamAccountName     : S-DC$

AD domain and forest information:
  Domain FQDN         : swansea.acca
  Domain GUID         : a9905b75-2efd-4ed7-8e78-a24b9c058190
  Domain NetBIOS Name : SWANSEA
  Domain SID          : S-1-5-21-3861473089-3053040122-1338177554
  Forest FQDN         : swansea.acca
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
192.168.1.1 resolves as S-DC.swansea.acca.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

  Content-Type: text/html
  Last-Modified: Fri, 26 Sep 2025 16:11:58 GMT
  Accept-Ranges: bytes
  ETag: "31e6e84802fdc1:0"
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Thu, 08 Jan 2026 21:54:33 GMT
  Content-Length: 34

Response Body :

<h1>Swansea ACCA VSite Page</h1>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
HTTP/2 TLS Support: Yes
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  WWW-Authenticate: NTLM
 TlRMTVNTUAACAAAADgAOADgAAAAFgokCrqhuOjKFQy8AAAAAAAAAAIwAjABGAAAACgB8TwAAAA9TAFcAQQBOAFMARQBBAAIADgBTAFcAQQBOAFMAR
+mA3AEAAAAA
  Date: Thu, 08 Jan 2026 21:54:32 GMT
  Content-Length: 341

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Authorized</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Authorized</h2>
<hr><p>HTTP Error 401. The requested resource requires user authentication.</p>
</BODY></HTML>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/5985/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Thu, 08 Jan 2026 21:54:33 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: b8048566478cf2e3f7df4605c61454d0
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Thu, 08 Jan 2026 21:54:32 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 1217
  Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self';
 frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src
 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self'
 www.tenable.com; object-src 'none'; base-uri 'self';
  Strict-Transport-Security: max-age=31536000; includeSubDomains
  Expect-CT: max-age=0
```

```
Response Body :

<!doctype html>
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-
src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src
 'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1760124798135" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=200e92783edd76dcdb599dd0c25b191f" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1760124798135"></script>
        <script src="p [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/47001/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Type: text/html; charset=us-ascii
  Server: Microsoft-HTTPAPI/2.0
  Date: Thu, 08 Jan 2026 21:54:33 GMT
  Connection: close
  Content-Length: 315

Response Body :
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/12/08

Plugin Output

tcp/0

```
+ Loopback Pseudo-Interface 1
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ IntSwa
  + IPv4
    - Address       : 192.168.1.1
      Assign Method : static
  + IPv6
    - Address       : fe80::3e44:49fe:e3f3:83e6%13
      Assign Method : dynamic
+ External
  + IPv4
    - Address       : 20.0.0.1
      Assign Method : static
  + IPv6
    - Address       : fe80::3183:de30:e5e8:b7d0%15
      Assign Method : dynamic
+ Internet
  + IPv4
    - Address       : 10.0.2.15
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::e147:b674:a231:8284%7
      Assign Method : dynamic
    - Address       : fd17:625c:f037:2:cfd0:7c37:27cc:3d7
      Assign Method : dynamic
```

179947 - Intel CPUID detection

Synopsis

The processor CPUID was detected on the remote host.

Description

The CPUID of the Intel processor was detected on the remote host.

See Also

https://www.intel.com

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/18, Modified: 2025/12/08

Plugin Output

tcp/135/epmap

```
Nessus was able to extract the following cpuid:
```

92421 - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://forensafe.com/blogs/typedurls.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2024/05/08

Plugin Output

tcp/0

```
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141

Internet Explorer typed URL report attached.
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/08, Modified: 2015/09/24

Plugin Output

tcp/88

```
Nessus gathered the following information :

  Server time  : 2026-01-08 21:52:07 UTC
  Realm        : SWANSEA.ACCA
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/07/12, Modified: 2022/09/28

Plugin Output

tcp/389/ldap

```
[+]-namingContexts:
   |  DC=swansea,DC=acca
   |  CN=Configuration,DC=swansea,DC=acca
   |  CN=Schema,CN=Configuration,DC=swansea,DC=acca
   |  DC=DomainDnsZones,DC=swansea,DC=acca
   |  DC=ForestDnsZones,DC=swansea,DC=acca
[+]-domainFunctionality:
   |  7
[+]-forestFunctionality:
   |  7
[+]-domainControllerFunctionality:
   |  7
[+]-rootDomainNamingContext:
   |  DC=swansea,DC=acca
[+]-ldapServiceName:
   |  swansea.acca:s-dc$@SWANSEA.ACCA
[+]-isGlobalCatalogReady:
   |  TRUE
[+]-supportedSASLMechanisms:
   |  GSSAPI
   |  GSS-SPNEGO
   |  EXTERNAL
   |  DIGEST-MD5
[+]-supportedLDAPVersion:
   |  3
   |  2
[+]-supportedLDAPPolicies:
   |  MaxPoolThreads
   |  MaxPercentDirSyncRequests
   |  MaxDatagramRecv
```

```
    |  MaxReceiveBuffer
    |  MaxPreAuthReceiveBuffer
    |  InitRecvTimeout
    |  MaxConnections
    |  MaxConnIdleTime
    |  MaxPageSize
    |  MaxBatchReturnMessages
    |  MaxQueryDuration
    |  MaxDirSyncDuration
    |  MaxTempTableSize
    |  MaxResultSetSize
    |  MinResultSets
    |  MaxResultSetsPerConn
    |  MaxNotificationPerConn
    |  MaxValRange
    |  MaxValRangeTransitive
    |  ThreadMemoryLimit
    |  SystemMemoryLimitPercent
[+]-supportedControl:
    |  1.2.840.113556.1.4.319
    |  1.2.840.113556.1.4.801
    |  1.2.840.113556.1.4.473
    |  1.2.840.113556.1.4.528
    |  1.2.840.113556.1.4.417
    |  1.2.840.113556.1.4.619
    |  1.2.840.113556.1.4.841
    |  1.2.840.113556.1.4.529
    |  1.2.840.113556.1.4.805
    |  1.2.840.113556.1.4.521
    |  1.2.840.113556.1.4.970
    |  1.2.840.113556.1.4.1338
    |  1.2.840.113556.1.4.474
    |  1.2.840.113556.1.4.1339
    |  1.2.840.113556.1.4.1340
    |  1.2.840.113556.1.4.1413
    |  2.16.840.1.113730.3.4.9
    |  2.16.840.1.113730.3.4.10
    |  1.2.840.113556.1.4.1504
    |  1.2.840.113556.1.4.1852
    |  1.2.840.113556.1.4.802
    |  1.2.840.113556.1.4.1907
    |  1.2.840.113556.1.4.1948
    |  1.2.840.113556.1.4.1974
    |  1.2.840.113556.1.4.1341
    |  1.2.840.113556.1.4.2026
    |  1.2.840.113556.1.4.2064
    |  1.2.840.113556.1.4.2065
    |  1.2.840.113556.1.4.2066
    |  1.2.840. [...]
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/07/12, Modified: 2022/09/28

Plugin Output

tcp/3268/ldap

```
[+]-namingContexts:
   |  DC=swansea,DC=acca
   |  CN=Configuration,DC=swansea,DC=acca
   |  CN=Schema,CN=Configuration,DC=swansea,DC=acca
   |  DC=DomainDnsZones,DC=swansea,DC=acca
   |  DC=ForestDnsZones,DC=swansea,DC=acca
[+]-domainFunctionality:
   |  7
[+]-forestFunctionality:
   |  7
[+]-domainControllerFunctionality:
   |  7
[+]-rootDomainNamingContext:
   |  DC=swansea,DC=acca
[+]-ldapServiceName:
   |  swansea.acca:s-dc$@SWANSEA.ACCA
[+]-isGlobalCatalogReady:
   |  TRUE
[+]-supportedSASLMechanisms:
   |  GSSAPI
   |  GSS-SPNEGO
   |  EXTERNAL
   |  DIGEST-MD5
[+]-supportedLDAPVersion:
   |  3
   |  2
[+]-supportedLDAPPolicies:
   |  MaxPoolThreads
   |  MaxPercentDirSyncRequests
   |  MaxDatagramRecv
```

```
    |  MaxReceiveBuffer
    |  MaxPreAuthReceiveBuffer
    |  InitRecvTimeout
    |  MaxConnections
    |  MaxConnIdleTime
    |  MaxPageSize
    |  MaxBatchReturnMessages
    |  MaxQueryDuration
    |  MaxDirSyncDuration
    |  MaxTempTableSize
    |  MaxResultSetSize
    |  MinResultSets
    |  MaxResultSetsPerConn
    |  MaxNotificationPerConn
    |  MaxValRange
    |  MaxValRangeTransitive
    |  ThreadMemoryLimit
    |  SystemMemoryLimitPercent
[+]-supportedControl:
    |  1.2.840.113556.1.4.319
    |  1.2.840.113556.1.4.801
    |  1.2.840.113556.1.4.473
    |  1.2.840.113556.1.4.528
    |  1.2.840.113556.1.4.417
    |  1.2.840.113556.1.4.619
    |  1.2.840.113556.1.4.841
    |  1.2.840.113556.1.4.529
    |  1.2.840.113556.1.4.805
    |  1.2.840.113556.1.4.521
    |  1.2.840.113556.1.4.970
    |  1.2.840.113556.1.4.1338
    |  1.2.840.113556.1.4.474
    |  1.2.840.113556.1.4.1339
    |  1.2.840.113556.1.4.1340
    |  1.2.840.113556.1.4.1413
    |  2.16.840.1.113730.3.4.9
    |  2.16.840.1.113730.3.4.10
    |  1.2.840.113556.1.4.1504
    |  1.2.840.113556.1.4.1852
    |  1.2.840.113556.1.4.802
    |  1.2.840.113556.1.4.1907
    |  1.2.840.113556.1.4.1948
    |  1.2.840.113556.1.4.1974
    |  1.2.840.113556.1.4.1341
    |  1.2.840.113556.1.4.2026
    |  1.2.840.113556.1.4.2064
    |  1.2.840.113556.1.4.2065
    |  1.2.840.113556.1.4.2066
    |  1.2.840. [...]
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

https://en.wikipedia.org/wiki/LDAP

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/02/10, Modified: 2022/09/29

Plugin Output

tcp/389/ldap

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

https://en.wikipedia.org/wiki/LDAP

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/02/10, Modified: 2022/09/29

Plugin Output

tcp/3268/ldap

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?51eae65d

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'S-DC'.
```

160301 - Link-Local Multicast Name Resolution (LLMNR) Service Detection

Synopsis

Verify status of the LLMNR service on the remote host.

Description

The Link-Local Multicast Name Resolution (LLMNR) service allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link

See Also

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2022/04/28, Modified: 2022/12/29

Plugin Output

tcp/445/cifs

```
LLMNR Key SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast not found.
```

22319 - MSRPC Service Detection

Synopsis

A DCE/RPC server is listening on the remote host.

Description

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.

However it is not possible to determine the uuid of this service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/09/11, Modified: 2019/09/25

Plugin Output

tcp/59349/dce-rpc

92424 - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
@%systemroot%\system32\themeservice.dll,-8192 : Themes
@%systemroot%\system32\tabsvc.dll,-100 : Touch Keyboard and Handwriting Panel Service
@%systemroot%\system32\mprmsg.dll,-32011 : Remote Access IP ARP Driver
@%systemroot%\system32\windows.devices.picker.dll,-1006 : DevicePicker
@firewallapi.dll,-50304 : Enables Simple Network Management Protocol (SNMP) requests to be processed
 by this computer. If this service is stopped, the computer will be unable to process SNMP requests.
 If this service is disabled, any services that explicitly depend on it will fail to start.
@%systemroot%\system32\bfe.dll,-1002 : The Base Filtering Engine (BFE) is a service that manages
 firewall and Internet Protocol security (IPsec) policies and implements user mode filtering.
 Stopping or disabling the BFE service will significantly reduce the security of the system. It will
 also result in unpredictable behavior in IPsec management and firewall applications.
c:\windows\system32,@elscore.dll,-8 : Microsoft Malayalam to Latin Transliteration
@%systemroot%\system32\lpdsvc.dll,-501 : Enables client computers to print to the Line Printer
 Daemon (LPD) service on this server using TCP/IP and the Line Printer Remote (LPR) protocol.
@%systemroot%\system32\browser.dll,-101 : Maintains an updated list of computers on the network and
 supplies this list to computers designated as browsers. If this service is stopped, this list will
 not be updated or maintained. If this service is disabled, any services that explicitly depend on
 it will fail to start.
@%systemroot%\system32\gatewayhealthmonitorservice.dll,-201 : Offers monitoring for the gateway
 health.
@%systemroot%\system32\devicesflowbroker.dll,-103 : DevicesFlow
```

```
@%systemroot%\system32\ias.dll,-1001 : Manages authentication, authorization, auditing and
 accounting for virtual private network (VPN), dial-up, 802.1x wireless or Ethernet switch
 connection attempts sent by access servers that are compatible with the IETF RADIUS protocol. If
 this service is stopped, users might be unable to obtain a VPN [...]
```

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net

http://www.nessus.org/u?15ae6806

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0655

Plugin Information

Published: 2010/12/20, Modified: 2025/10/15

Plugin Output

tcp/445/cifs

```
Nessus detected 2 installs of Microsoft .NET Framework:

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.04161
  Install Type : Full
  Release      : 528449

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.04161
  Install Type : Client
  Release      : 528449
```

99364 - Microsoft .NET Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft .NET security rollups.

Description

Nessus was able to enumerate the Microsoft .NET security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?662e30c9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/14, Modified: 2025/10/23

Plugin Output

tcp/445/cifs

```
Path                          : C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
Version                       : 4.8.4775.0
.NET Version                  : 4.8
Associated KB                 : 5049617
Latest effective update level : 01_2025
```

176212 - Microsoft Edge Add-on Enumeration (Windows)

Synopsis

One or more Microsoft Egde browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Microsoft Edge browser extensions installed on the remote host.

See Also

https://microsoftedge.microsoft.com/addons

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/05/22, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
User : Administrator
|- Browser : Microsoft Edge
  |- Add-on information :

    Name    : unknown
    Version : 1.97.1
    Path    : C:\Users\Administrator\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.97.1_0

    Name    : unknown
    Version : 1.99.1
    Path    : C:\Users\Administrator\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.99.1_0

    Name        : Edge relevant text changes
    Description : Edge relevant text changes on select websites to improve user experience and
 precisely surfaces the action they want to take.
    Version     : 1.2.1
    Path        : C:\Users\Administrator\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\jmjflgjpcpepeafmmgdpfkogkghcpiha\1.2.1_0
```

136969 - Microsoft Edge Chromium Installed

Synopsis

Microsoft Edge (Chromium-based) is installed on the remote host.

Description

Microsoft Edge (Chromium-based), a Chromium-based web browser, is installed on the remote host.

See Also

https://www.microsoft.com/en-us/edge

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/29, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 143.0.3650.96
Channel : stable
```

72879 - Microsoft Internet Explorer Enhanced Security Configuration Detection

Synopsis

The remote host supports IE Enhanced Security Configuration.

Description

Nessus detects if the remote Windows host supports IE Enhanced Security Configuration (ESC) and if IE ESC features are enabled or disabled.

See Also

http://www.nessus.org/u?a9c4c131

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/03/07, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Type       : Admin Groups
Is Enabled : True

Type       : User Groups
Is Enabled : True
```

162560 - Microsoft Internet Explorer Installed

Synopsis

A web browser is installed on the remote Windows host.

Description

Microsoft Internet Explorer, a web browser bundled with Microsoft Windows, is installed on the remote Windows host.

See Also

https://support.microsoft.com/products/internet-explorer

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/06/28, Modified: 2025/12/08

Plugin Output

tcp/0

```
Path    : C:\Windows\system32\mshtml.dll
Version : 11.0.20348.4050
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

https://support.microsoft.com/en-us/help/17621/internet-explorer-downloads

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0509

Plugin Information

Published: 2014/02/06, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Version  : 11.1.20348.0
```

139615 - Microsoft Internet Information Services (IIS) Installed

Synopsis

Checks Windows registry keys and executables for a Microsoft Internet Information Services (IIS) installation.

Description

Microsoft Internet Information Services installation (IIS) has been detected on the remote Windows host.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0944

Plugin Information

Published: 2020/08/17, Modified: 2025/12/08

Plugin Output

tcp/0

```
Path    : C:\Windows\system32\inetsrv
Version : 10.0.20348.2849
```

140655 - Microsoft Internet Information Services (IIS) Sites Enumeration

Synopsis

Checks IIS configuration file for configured sites and their bound addresses.

Description

Microsoft Internet Information Services configuration file has been parsed to extract information about the existing sites, their protocols, domains and IP addresses.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/09/18, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Nessus found the following sites configured on the remote host:
+ site name: VFTP
  + binding 0
    - IP address : *
    - port       : 21
    - domain     :
    - protocol   : ftp
+ site name: VSite
  + binding 0
    - IP address : *
    - port       : 80
    - domain     :
    - protocol   : http
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates.

Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/06, Modified: 2021/07/12

Plugin Output

tcp/445/cifs

```
Nessus is able to test for missing patches using :
  Nessus
```

125835 - Microsoft Remote Desktop Connection Installed

Synopsis

A graphical interface connection utility is installed on the remote Windows host

Description

Microsoft Remote Desktop Connection (also known as Remote Desktop Protocol or Terminal Services Client) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?1c33f0e7

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/06/12, Modified: 2022/10/10

Plugin Output

tcp/0

```
Path    : C:\Windows\\System32\\mstsc.exe
Version : 10.0.20348.2849
```

11217 - Microsoft SQL Server Detection (credentialed check)

Synopsis

The remote host has a database server installed.

Description

Nessus has detected one or more installs of Microsoft SQL server by examining the registry and file systems on the remote host.

See Also

http://www.nessus.org/u?e45407e9

Solution

Ensure the latest service pack and hotfixes are installed.

Risk Factor

None

References

XREF IAVT:0001-T-0800

Plugin Information

Published: 2003/01/26, Modified: 2025/09/24

Plugin Output

tcp/445/cifs

```
  Path                : C:\Windows\WID\Binn\
  Version             : 12.0.5214.6
  arch                : x64
  instance_name       : MSWIN8.SQLWID
  is_accessible_share : 1
  local_db            : 0
  localdb             : 0

  Version             : 12.0.5214.6
  Edition             : Windows Internal Database (64-bit)
  Path                : C:\Windows\WID\Binn\
  Named Instance      : MSWIN8.SQLWID
  Recommended Version : 12.0.6439.10 (2014 + SP3 CU4 Security Update June 2022 (KB5014164)).
```

93962 - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/10/11, Modified: 2025/11/18

Plugin Output

tcp/445/cifs

```
Cumulative Rollup : 08_2025 [KB5063880]
Cumulative Rollup : 07_2025
Cumulative Rollup : 06_2025
Cumulative Rollup : 05_2025
Cumulative Rollup : 04_2025
Cumulative Rollup : 03_2025
Cumulative Rollup : 02_2025
Cumulative Rollup : 01_2025
Cumulative Rollup : 12_2024
Cumulative Rollup : 11_2024
Cumulative Rollup : 10_2024
Cumulative Rollup : 09_2024
Cumulative Rollup : 08_2024
Cumulative Rollup : 07_2024
Cumulative Rollup : 06_2024
Cumulative Rollup : 05_2024
Cumulative Rollup : 04_2024
Cumulative Rollup : 03_2024
Cumulative Rollup : 02_2024
Cumulative Rollup : 01_2024
Cumulative Rollup : 12_2023
Cumulative Rollup : 11_2023
Cumulative Rollup : 10_2023
Cumulative Rollup : 09_2023
```

```
  Cumulative Rollup : 08_2023
  Cumulative Rollup : 07_2023
  Cumulative Rollup : 06_2023
  Cumulative Rollup : 05_2023
  Cumulative Rollup : 04_2023
  Cumulative Rollup : 03_2023
  Cumulative Rollup : 02_2023
  Cumulative Rollup : 01_2023
  Cumulative Rollup : 12_2022
  Cumulative Rollup : 11_2022
  Cumulative Rollup : 10_2022
  Cumulative Rollup : 09_2022
  Cumulative Rollup : 08_2022
  Cumulative Rollup : 07_2022
  Cumulative Rollup : 06_2022
  Cumulative Rollup : 05_2022
  Cumulative Rollup : 04_2022
  Cumulative Rollup : 03_2022
  Cumulative Rollup : 02_2022
  Cumulative Rollup : 01_2022
  Cumulative Rollup : 12_2021
  Cumulative Rollup : 11_2021
  Cumulative Rollup : 10_2021

  Latest effective update level : 08_2025
  File checked                  : C:\Windows\system32\ntoskrnl.exe
  File version                  : 10.0.20348.4050
  Associated KB                 : 5063880
```

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information

Published: 2002/03/15, Modified: 2018/05/16

Plugin Output

tcp/445/cifs

```
The following users are members of the 'Administrators' group :

  - SWANSEA\Administrator (User)
  - SWANSEA\Enterprise Admins (Group)
  - SWANSEA\Domain Admins (Group)
```

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

CWDIllegalInDllSearch Settings: Improper settings could allow code execution attacks.

Description

Windows Hosts can be hardened against DLL hijacking attacks by setting the The 'CWDIllegalInDllSearch' registry entry in to one of the following settings:

- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)

- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)

- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

http://www.nessus.org/u?0c574c56

http://www.nessus.org/u?5234ef0c

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/26, Modified: 2019/12/20

Plugin Output

tcp/445/cifs

```
Name  : SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch
Value : Registry Key Empty or Missing
```

92370 - Microsoft Windows ARP Table

Synopsis

Nessus was able to collect and report ARP table information from the remote host.

Description

Nessus was able to collect ARP table information from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/12/08

Plugin Output

tcp/0

```
10.0.2.2 : 52-55-0a-00-02-02
10.0.2.255 : ff-ff-ff-ff-ff-ff
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa
255.255.255.255 : ff-ff-ff-ff-ff-ff
192.168.1.2 : 08-00-27-1f-fc-7b
192.168.1.10 : 08-00-27-ae-45-d6
192.168.1.255 : ff-ff-ff-ff-ff-ff
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa
255.255.255.255 : ff-ff-ff-ff-ff-ff
20.0.0.3 : ff-ff-ff-ff-ff-ff
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa

Extended ARP table information attached.
```

92371 - Microsoft Windows DNS Cache

Synopsis

Nessus was able to collect and report DNS cache information from the remote host.

Description

Nessus was able to collect details of the DNS cache from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/12/08

Plugin Output

tcp/0

```
    _ldap._tcp.default-first-site-name._sites.dc._msdcs.swansea.acca
    plugins.nessus.org
    plugins.nessus.org

DNS cache information attached.
```

92364 - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0757

Plugin Information

Published: 2016/07/19, Modified: 2022/06/24

Plugin Output

tcp/0

```
Global Environment Variables :
  processor_level : 23
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 2
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 7100
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : AMD64 Family 23 Model 113 Stepping 0, AuthenticAMD
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-3861473089-3053040122-1338177554-500
    temp : %USERPROFILE%\AppData\Local\Temp
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
```

```
    tmp : %USERPROFILE%\AppData\Local\Temp
```

92365 - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2020/01/27

Plugin Output

tcp/0

```
Windows hosts file attached.

MD5: 3688374325b992def12793500307566d
SHA-1: 4bed0823746a2a8577ab08ac8711b79770e48274
SHA-256: 2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085
```

187318 - Microsoft Windows Installed

Synopsis

The remote host is running Microsoft Windows.

Description

The remote host is running Microsoft Windows.

See Also

https://www.microsoft.com/en-us/windows

https://www.microsoft.com/en-us/windows-server

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/12/27, Modified: 2025/09/29

Plugin Output

tcp/0

```
OS Name      : Microsoft Windows Server 2022 21H2
Vendor       : Microsoft
Product      : Windows Server
Release      : 2022 21H2
Edition      : Datacenter
Version      : 10.0.20348.4052
Role         : server
Kernel       : Windows NT 10.0
Architecture : x64
CPE v2.2     : cpe:/o:microsoft:windows_server_2022:10.0.20348.4052:-:~~datacenter~~x64~
CPE v2.3     : cpe:2.3:o:microsoft:windows_server_2022:10.0.20348.4052:-:*:*:datacenter:*:x64:*
Type         : local
Method       : SMB
Confidence   : 100
```

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates

Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0501

Plugin Information

Published: 2006/01/26, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
The following software are installed on the remote host :

Google Chrome  [version 143.0.7499.170]  [installed on 2026/01/06]
Microsoft Edge  [version 143.0.3650.96]  [installed on 2026/01/05]
Microsoft Edge Update  [version 1.3.215.9]
Npcap OEM  [version 1.72]
Tenable Nessus (x64)  [version 10.10.0.20152]  [installed on 2025/10/27]
```

178102 - Microsoft Windows Installed Software Version Enumeration

Synopsis

Enumerates installed software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.

Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2023/07/10, Modified: 2024/07/15

Plugin Output

tcp/445/cifs

```
The following software information is available on the remote host :

 - Npcap OEM
     Best Confidence Version  : 5.1.72.1206
     Version Confidence Level : 3
     All Possible Versions    :  5.1.72.1206, 1.72
     Other Version Data
       [VersionMajor] :
           Raw Value           : 1
       [InstallLocation] :
           Raw Value           : C:\Program Files\Npcap
       [DisplayName] :
           Raw Value           : Npcap OEM
       [UninstallString] :
           Raw Value           : "C:\Program Files\Npcap\uninstall.exe"
           Parsed File Path    : C:\Program Files\Npcap\uninstall.exe
           Parsed File Version : 5.1.72.1206
       [DisplayVersion] :
           Raw Value           : 1.72
       [VersionMinor] :
           Raw Value           : 72
       [DisplayIcon] :
```

```
          Raw Value           : C:\Program Files\Npcap\uninstall.exe
          Parsed File Path    : C:\Program Files\Npcap\uninstall.exe
          Parsed File Version : 5.1.72.1206

- Tenable Nessus (x64)
    Best Confidence Version  : 10.10.0.20152
    Version Confidence Level : 2
    All Possible Versions    :  10.10.0.20152
    Other Version Data
      [InstallDate] :
          Raw Value           : 2025/10/27
      [InstallLocation] :
          Raw Value           : C:\Program Files\Tenable\Nessus\
      [UninstallString] :
          Raw Value           : MsiExec.exe /X{FEEA2C81-3E50-4A83-89A3-1ED7AEE8407F}
      [VersionMinor] :
          Raw Value           : 10
      [Version] :
          Raw Value           : 168427520
      [VersionMajor] :
          Raw Value           : 10
      [Publisher] :
          Raw Value           : Tenable, Inc.
      [DisplayVersion] :
          Raw Value           : 10.10.0.20152
      [DisplayName] :
          Raw Value           : Tenable Nessus (x64)

- Google Chrome
    Best Confidence Version  : 143.0.7499.170
    Version Confidence Level : 3
    All Possible Versions    :  143.0.7499.170
    Other Version Data
      [InstallDate] : [...]
```

92366 - Microsoft Windows Last Boot Time

Synopsis

Nessus was able to collect the remote host's last boot time in a human readable format.

Description

Nessus was able to collect and report the remote host's last boot time as an ISO 8601 timestamp.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/07/09

Plugin Output

tcp/0

```
Last reboot : 2026-01-08T21:25:55+00:00 (20260108212555.500000+000)
```

161502 - Microsoft Windows Logged On Users

Synopsis

Nessus was able to determine the logged on users from the registry

Description

Using the HKU registry, Nessus was able to enumerate the SIDs of logged on users

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/05/25, Modified: 2025/10/01

Plugin Output

tcp/445/cifs

```
Logged on users :
  - S-1-5-21-3861473089-3053040122-1338177554-500
    Domain   : SWANSEA
    Username : Administrator
```

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?99fcc329

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2012/11/28, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
  Name     : \dosdevices\e:
  Data     : DMIO:ID:>0%Dd<
  Raw data : 444d494f3a49443a81963e183025194485edbe649e3c0ba0

  Name     : \dosdevices\d:
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f00580026005000720 06f006400 5

  Name     : \??\volume{fbb5c784-99a2-11f0-93d8-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f00580026005000720 06f006400 5

  Name     : \dosdevices\c:
  Data     : /&P
  Raw data : 2f26f9fe0000500600000000
```

92372 - Microsoft Windows NetBIOS over TCP/IP Info

Synopsis

Nessus was able to collect and report NBT information from the remote host.

Description

Nessus was able to collect details for NetBIOS over TCP/IP from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/12/08

Plugin Output

tcp/0

```
NBT information attached.
First 10 lines of all CSVs:
nbtstat_local.csv:
Interface,Name,Suffix,Type,Status,MAC
10.0.2.15,S-DC,<00>,UNIQUE,Registered,08:00:27:1A:80:9D
10.0.2.15,SWANSEA,<00>,GROUP,Registered,08:00:27:1A:80:9D
10.0.2.15,SWANSEA,<1C>,GROUP,Registered,08:00:27:1A:80:9D
10.0.2.15,S-DC,<20>,UNIQUE,Registered,08:00:27:1A:80:9D
10.0.2.15,SWANSEA,<1E>,GROUP,Registered,08:00:27:1A:80:9D
10.0.2.15,SWANSEA,<1B>,UNIQUE,Registered,08:00:27:1A:80:9D
10.0.2.15,SWANSEA,<1D>,UNIQUE,Registered,08:00:27:1A:80:9D
10.0.2.15,..__MSBROWSE__.,<01>,GROUP,Registered,08:00:27:1A:80:9D
192.168.1.1,S-DC,<00>,UNIQUE,Registered,08:00:27:2A:B5:B6
192.168.1.1,SWANSEA,<00>,GROUP,Registered,08:00:27:2A:B5:B6
```

103871 - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0758

Plugin Information

Published: 2017/10/17, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Network Adapter Driver Description : Intel(R) PRO/1000 MT Desktop Adapter
Network Adapter Driver Version     : 8.4.13.0

Network Adapter Driver Description : Intel(R) PRO/1000 MT Desktop Adapter
Network Adapter Driver Version     : 8.4.13.0

Network Adapter Driver Description : Intel(R) PRO/1000 MT Desktop Adapter
Network Adapter Driver Version     : 8.4.13.0
```

65791 - Microsoft Windows Portable Devices

Synopsis

It is possible to get a list of portable devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates portable devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?af102b66

Solution

Make sure that use of the portable devices agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Friendly name : E:\
Device        : SWD#WPDBUSENUM#{84826F67-9C08-11F0-93EF-0800274BBFAA}#0000000008100000

Friendly name : Apple iPhone
Device        : USB#VID_05AC&PID_12A8#0000812000146C4A3644201E
```

92367 - Microsoft Windows PowerShell Execution Policy

Synopsis

Nessus was able to collect and report the PowerShell execution policy for the remote host.

Description

Nessus was able to collect and report the PowerShell execution policy for the remote Windows host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2020/06/12

Plugin Output

tcp/0

```
HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy : RemoteSigned
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy :
 RemoteSigned
```

151440 - Microsoft Windows Print Spooler Service Enabled

Synopsis

The Microsoft Windows Print Spooler service on the remote host is enabled.

Description

The Microsoft Windows Print Spooler service (spoolsv.exe) on the remote host is enabled.

See Also

http://www.nessus.org/u?8fc5df24

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/07, Modified: 2021/07/07

Plugin Output

tcp/445/cifs

```
The Microsoft Windows Print Spooler service on the remote host is enabled.
```

70329 - Microsoft Windows Process Information

Synopsis

Use WMI to obtain running process information.

Description

Report details on the running processes on the machine.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/08, Modified: 2025/12/08

Plugin Output

tcp/0

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (312)
 0 : Registry (100)
 0 : csrss.exe (408)
 1 : csrss.exe (480)
 0 : wininit.exe (488)
 0 : |- services.exe (620)
 0 :    |- svchost.exe (1072)
 0 :    |- svchost.exe (1096)
 0 :    |- svchost.exe (1112)
 0 :    |- svchost.exe (1208)
 0 :    |- svchost.exe (1228)
 0 :    |- inetinfo.exe (1272)
 0 :    |- svchost.exe (1276)
 0 :    |- svchost.exe (1284)
 0 :    |- svchost.exe (1304)
 0 :    |- svchost.exe (1324)
 0 :    |- svchost.exe (1400)
 0 :    |- svchost.exe (1424)
 0 :    |- svchost.exe (1476)
 0 :    |- svchost.exe (1504)
 0 :    |- svchost.exe (1584)
 0 :    |- svchost.exe (1596)
 1 :       |- taskhostw.exe (4788)
 0 :    |- svchost.exe (1620)
```

```
0 :    |- svchost.exe (1688)
1 :       |- sihost.exe (2804)
0 :    |- Microsoft.ActiveDirectory.WebServices.exe (1724)
0 :    |- svchost.exe (1760)
0 :    |- svchost.exe (1768)
0 :    |- svchost.exe (1788)
0 :    |- svchost.exe (1808)
0 :    |- svchost.exe (1864)
0 :    |- svchost.exe (1868)
0 :    |- svchost.exe (1880)
0 :    |- svchost.exe (1940)
0 :    |- svchost.exe (1988)
0 :    |- svchost.exe (2212)
0 :    |- svchost.exe (2216)
0 :    |- svchost.exe (2224)
0 :    |- svchost.exe (2232)
0 :    |- svchost.exe (2488)
0 :    |- svchost.exe (2588)
0 :    |- spoolsv.exe (2736)
0 :    |- svchost.exe (2740)
0 :    |- svchost.exe (2812)
0 :    |- svchost.exe (2836)
0 :    |- svchost.exe (2888)
0 :    |- svchost.exe (2900)
0 :    |- dfsrs.exe (2932)
0 :    |- svchost.exe (2972)
0 :    |- dns.exe (3012)
0 :    |- svchost.exe (3028)
0 :       |- AggregatorHost.exe (4484)
0 :    |- ismserv.exe (3080)
0 :    |- svchost.exe (3108)
0 :    |- svchost.exe (3152)
0 :    |- dfssvc.exe (3192)
0 :    |- MpDefenderCoreService.exe (3224)
0 :    |- msdtc.exe (328)
0 :    |- svchost.exe (3284)
0 :    |- TCPSVCS.EXE (3300)
0 :    |- svchost.exe (3308)
0 :    |- snmp.exe (3312)
[...]
```

70331 - Microsoft Windows Process Module Information

Synopsis

Use WMI to obtain running process module information.

Description

Report details on the running processes modules on the machine.

This plugin is informative only and could be used for forensic investigation, malware detection, and to that confirm your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/08, Modified: 2025/12/08

Plugin Output

tcp/0

```
Process_Modules_.csv : lists the loaded modules for each process.
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/7/echo

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/7

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/9/discard

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/9

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/13/daytime

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/13/daytime

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/17/qotd

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/17/qotd

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/19/chargen

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/19

```
The Win32 process 'TCPSVCS.EXE' is listening on this port (pid 3300).

This process 'TCPSVCS.EXE' (pid 3300) is hosting the following Windows services :
simptcp (@%SystemRoot%\system32\simptcp.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/21/ftp

```
The Win32 process 'svchost.exe' is listening on this port (pid 1400).

This process 'svchost.exe' (pid 1400) is hosting the following Windows services :
ftpsvc (@%windir%\system32\inetsrv\ftpres.dll,-30001)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/53/dns

```
The Win32 process 'dns.exe' is listening on this port (pid 3012).

This process 'dns.exe' (pid 3012) is hosting the following Windows services :
DNS (@%systemroot%\system32\dns.exe,-49157)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/53/dns

```
The Win32 process 'dns.exe' is listening on this port (pid 3012).

This process 'dns.exe' (pid 3012) is hosting the following Windows services :
DNS (@%systemroot%\system32\dns.exe,-49157)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/67

```
The Win32 process 'svchost.exe' is listening on this port (pid 2740).

This process 'svchost.exe' (pid 2740) is hosting the following Windows services :
DHCPServer (@%SystemRoot%\system32\dhcpssvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/68

```
The Win32 process 'svchost.exe' is listening on this port (pid 2740).

This process 'svchost.exe' (pid 2740) is hosting the following Windows services :
DHCPServer (@%SystemRoot%\system32\dhcpssvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/80/www

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/88

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/88

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/123/ntp

```
The Win32 process 'svchost.exe' is listening on this port (pid 820).

This process 'svchost.exe' (pid 820) is hosting the following Windows services :
W32Time (@%SystemRoot%\system32\w32time.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/135/epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 936).

This process 'svchost.exe' (pid 936) is hosting the following Windows services :
RpcEptMapper (@%windir%\system32\RpcEpMap.dll,-1001)
RpcSs (@combase.dll,-5010)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/137/netbios-ns

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/138

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/139/smb

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/161

```
The Win32 process 'snmp.exe' is listening on this port (pid 3312).

This process 'snmp.exe' (pid 3312) is hosting the following Windows services :
SNMP (@firewallapi.dll,-50303)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/389/ldap

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/389

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/443/www

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/464

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/464

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/500

```
The Win32 process 'svchost.exe' is listening on this port (pid 2216).

This process 'svchost.exe' (pid 2216) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/515

```
The Win32 process 'svchost.exe' is listening on this port (pid 3152).

This process 'svchost.exe' (pid 3152) is hosting the following Windows services :
LPDSVC (@%systemroot%\system32\lpdsvc.dll,-500)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/593/http-rpc-epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 936).

This process 'svchost.exe' (pid 936) is hosting the following Windows services :
RpcEptMapper (@%windir%\system32\RpcEpMap.dll,-1001)
RpcSs (@combase.dll,-5010)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/636

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/1645

```
The Win32 process 'svchost.exe' is listening on this port (pid 504).

This process 'svchost.exe' (pid 504) is hosting the following Windows services :
IAS (@%SystemRoot%\system32\ias.dll,-1000)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/1646

```
The Win32 process 'svchost.exe' is listening on this port (pid 504).

This process 'svchost.exe' (pid 504) is hosting the following Windows services :
IAS (@%SystemRoot%\system32\ias.dll,-1000)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/1812

```
The Win32 process 'svchost.exe' is listening on this port (pid 504).

This process 'svchost.exe' (pid 504) is hosting the following Windows services :
IAS (@%SystemRoot%\system32\ias.dll,-1000)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/1813

```
The Win32 process 'svchost.exe' is listening on this port (pid 504).

This process 'svchost.exe' (pid 504) is hosting the following Windows services :
IAS (@%SystemRoot%\system32\ias.dll,-1000)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/2535

```
The Win32 process 'svchost.exe' is listening on this port (pid 2740).

This process 'svchost.exe' (pid 2740) is hosting the following Windows services :
DHCPServer (@%SystemRoot%\system32\dhcpssvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/3268/ldap

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/3269

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/3388/ncacn_http

```
The Win32 process 'svchost.exe' is listening on this port (pid 1096).

This process 'svchost.exe' (pid 1096) is hosting the following Windows services :
TSGateway (@%SystemRoot%\system32\aaedge.dll,-2002)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/3391

```
The Win32 process 'svchost.exe' is listening on this port (pid 1096).

This process 'svchost.exe' (pid 1096) is hosting the following Windows services :
TSGateway (@%SystemRoot%\system32\aaedge.dll,-2002)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/3702

```
The Win32 process 'svchost.exe' is listening on this port (pid 2588).

This process 'svchost.exe' (pid 2588) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/4500

```
The Win32 process 'svchost.exe' is listening on this port (pid 2216).

This process 'svchost.exe' (pid 2216) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/5353

```
The Win32 process 'svchost.exe' is listening on this port (pid 1228).

This process 'svchost.exe' (pid 1228) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/5355/llmnr

```
The Win32 process 'svchost.exe' is listening on this port (pid 1228).

This process 'svchost.exe' (pid 1228) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/5357/www

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/5504/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 3912).

This process 'svchost.exe' (pid 3912) is hosting the following Windows services :
TScPubRPC (@%SystemRoot%\System32\TSCPUBSvr.dll,-109)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/5985/www

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/8834/www

```
The Win32 process 'nessusd.exe' is listening on this port (pid 4460).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/9389

```
The Win32 process 'Microsoft.ActiveDirectory.WebServices.exe' is listening on this port (pid 1724).

This process 'Microsoft.ActiveDirectory.WebServices.exe' (pid 1724) is hosting the following Windows
 services :
ADWS (@%SystemRoot%\ADWS\adwsres.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/47001/www

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/49664/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/49665/dce-rpc

```
The Win32 process 'wininit.exe' is listening on this port (pid 488).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/49666/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1208).

This process 'svchost.exe' (pid 1208) is hosting the following Windows services :
EventLog (@%SystemRoot%\system32\wevtsvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/49667/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1596).

This process 'svchost.exe' (pid 1596) is hosting the following Windows services :
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/49668/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/54401/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 2224).

This process 'svchost.exe' (pid 2224) is hosting the following Windows services :
PolicyAgent (@%SystemRoot%\System32\polstore.dll,-5010)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

udp/56422

```
The Win32 process 'svchost.exe' is listening on this port (pid 2588).

This process 'svchost.exe' (pid 2588) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/59349/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 3500).

This process 'svchost.exe' (pid 3500) is hosting the following Windows services :
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64492/ncacn_http

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64493/dce-rpc

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 2736).

This process 'spoolsv.exe' (pid 2736) is hosting the following Windows services :
Spooler (@%systemroot%\system32\spoolsv.exe,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64499/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 2740).

This process 'svchost.exe' (pid 2740) is hosting the following Windows services :
DHCPServer (@%SystemRoot%\system32\dhcpssvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64509/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
Kdc (@%SystemRoot%\System32\kdcsvc.dll,-1)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
NTDS (@%SystemRoot%\System32\ntdsmsg.dll,-1)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64539/dce-rpc

```
The Win32 process 'dfsrs.exe' is listening on this port (pid 2932).

This process 'dfsrs.exe' (pid 2932) is hosting the following Windows services :
DFSR (@dfsrress.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64558/dce-rpc

```
The Win32 process 'services.exe' is listening on this port (pid 620).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64559/dce-rpc

```
The Win32 process 'tssdis.exe' is listening on this port (pid 6008).

This process 'tssdis.exe' (pid 6008) is hosting the following Windows services :
Tssdis (@%SystemRoot%\System32\tssdis.exe,-1026)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/12/08

Plugin Output

tcp/64639/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 3308).

This process 'svchost.exe' (pid 3308) is hosting the following Windows services :
RPCHTTPLBS (@%systemroot%\system32\RpcProxy\RpcProxy.dll,-2)
```

126527 - Microsoft Windows SAM user enumeration

Synopsis

Nessus was able to enumerate domain users from the local SAM.

Description

Using the domain security identifier (SID), Nessus was able to enumerate the domain users on the remote Windows system using the Security Accounts Manager.

Note: Unable to obtain SMB SAMR user data during Agent scans.

Rendering User data obtained by plugin 171956

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/07/08, Modified: 2025/06/04

Plugin Output

tcp/0

```
  - Administrator (id S-1-5-21-3861473089-3053040122-500, Built-in account for administering the
 computer/domain, Administrator account)
  - ftpuser (id S-1-5-21-3861473089-3053040122-1111)
  - Guest (id S-1-5-21-3861473089-3053040122-501, Built-in account for guest access to the computer/
domain, Guest account)
  - krbtgt (id S-1-5-21-3861473089-3053040122-502, Kerberos account, Key Distribution Center Service
 Account)
  - nitheesh (id S-1-5-21-3861473089-3053040122-1110, Nitheesh Murugan)
  - user1 (id S-1-5-21-3861473089-3053040122-1109, user1 user)
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

```
The following password policy is defined on the remote host:

Minimum password len: 4
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 0
Time between failed logon (s): 0
Number of invalid logon before locked out (s): 0
```

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.

Microsoft documentation notes that interactive console logons change the DefaultUserName registry entry to be the last logged-on user.

See Also

http://www.nessus.org/u?a29751b5

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/05/05, Modified: 2019/09/02

Plugin Output

tcp/445/cifs

```
Last Successful logon : SWANSEA\Administrator
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2025/07/21

Plugin Output

tcp/445/cifs

```
- The SMB tests will be done as SWANSEA\Administrator/******
- NULL sessions may be enabled on the remote host.
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-3861473089-3053040122-1338177554

The value of 'RestrictAnonymous' setting is : 0
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server 2022 Datacenter 20348
The remote native LAN manager is : Windows Server 2022 Datacenter 6.3
The remote SMB Domain Name is : SWANSEA
```

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/31, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Operating system version = 10.20348
Architecture = x64
Build lab extended = 20348.1.amd64fre.fe_release.210507-1500
```

10413 - Microsoft Windows SMB Registry : Remote PDC/BDC Detection

Synopsis

The remote system is a Domain Controller.

Description

The remote host seems to be a Primary Domain Controller or a Backup Domain Controller.

This can be verified by the value of the registry key 'ProductType'
under 'HKLM\SYSTEM\CurrentControlSet\Control\ProductOptions'.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0942

Plugin Information

Published: 2000/05/20, Modified: 2023/08/17

Plugin Output

tcp/445/cifs

11457 - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0. Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).

Cached logon credentials could be accessed by an attacker and subjected to brute force attacks.

See Also

http://www.nessus.org/u?184d3eab

http://www.nessus.org/u?fe16cea8

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Consult Microsoft documentation and best practices.

Risk Factor

None

Plugin Information

Published: 2003/03/24, Modified: 2018/06/05

Plugin Output

tcp/445/cifs

```
Max cached logons : 10
```

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

References

XREF IAVT:0001-T-0752

Plugin Information

Published: 2010/02/05, Modified: 2022/05/16

Plugin Output

tcp/445/cifs

```
The following services are set to start automatically :

  ADWS startup parameters :
    Display name : Active Directory Web Services
    Service name : ADWS
    Log on as : LocalSystem
    Executable path : C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe

  AppHostSvc startup parameters :
    Display name : Application Host Helper Service
    Service name : AppHostSvc
    Log on as : localSystem
    Executable path : C:\Windows\system32\svchost.exe -k apphost

  BFE startup parameters :
    Display name : Base Filtering Engine
    Service name : BFE
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
    Dependencies : RpcSs/

  BrokerInfrastructure startup parameters :
    Display name : Background Tasks Infrastructure Service
```

```
    Service name : BrokerInfrastructure
    Log on as : LocalSystem
    Executable path : C:\Windows\system32\svchost.exe -k DcomLaunch -p
    Dependencies : RpcEptMapper/DcomLaunch/RpcSs/

  CDPSvc startup parameters :
    Display name : Connected Devices Platform Service
    Service name : CDPSvc
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalService -p
    Dependencies : ncbservice/RpcSS/Tcpip/

  CDPUserSvc_277d36 startup parameters :
    Display name : Connected Devices Platform User Service_277d36
    Service name : CDPUserSvc_277d36
    Executable path : C:\Windows\system32\svchost.exe -k UnistackSvcGroup

  CoreMessagingRegistrar startup parameters :
    Display name : CoreMessaging
    Service name : CoreMessagingRegistrar
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
    Dependencies : rpcss/

  CryptSvc startup parameters :
    Display name : Cryptographic Services
    Service name : CryptSvc
    Log on as : NT Authority\NetworkService
    Executable path : C:\Windows\system32\svchost.exe -k NetworkService -p
    Dependencies : RpcSs/

  DFSR startup parame [...]
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.

An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0751

Plugin Information

Published: 2000/07/03, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Active Services :

Active Directory Web Services [ ADWS ]
Application Host Helper Service [ AppHostSvc ]
Base Filtering Engine [ BFE ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Computer Browser [ Browser ]
Capability Access Manager Service [ camsvc ]
Connected Devices Platform Service [ CDPSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Association Service [ DeviceAssociationService ]
DFS Namespace [ Dfs ]
DFS Replication [ DFSR ]
DHCP Client [ Dhcp ]
DHCP Server [ DHCPServer ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
DNS Server [ DNS ]
```

```
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Function Discovery Provider Host [ fdPHost ]
Function Discovery Resource Publication [ FDResPub ]
Windows Font Cache Service [ FontCache ]
Microsoft FTP Service [ ftpsvc ]
Group Policy Client [ gpsvc ]
Network Policy Server [ IAS ]
IIS Admin Service [ IISADMIN ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
IP Helper [ iphlpsvc ]
Intersite Messaging [ IsmServ ]
Kerberos Key Distribution Center [ Kdc ]
CNG Key Isolation [ KeyIso ]
KDC Proxy Server service (KPS) [ KPSSVC ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
TCP/IP NetBIOS Helper [ lmhosts ]
LPD Service [ LPDSVC ]
Local Session Manager [ LSM ]
Microsoft Defender Core Service [ MDCoreSvc ]
Windows Defender Firewall [ mpssvc ]
Distributed Transaction Coordinator [ MSDTC ]
Windows Internal Database [ MSSQL$MICROSOFT##WID ]
Network Connection Broker [ NcbService ]
Netlogon [ Netlogon ]
Network List Service [ netprofm ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Active Directory Domain Services [ NTDS ]
Program Compatibility Assistant Service [ PcaSvc ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Prof [...]
```

92373 - Microsoft Windows SMB Sessions

Synopsis

Nessus was able to collect and report SMB session information from the remote host.

Description

Nessus was able to collect details of SMB sessions from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/12/08

Plugin Output

tcp/0

```
Administrator

Extended SMB session information attached.
```

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information

Published: 2007/01/04, Modified: 2011/03/21

Plugin Output

tcp/445/cifs

```
Here is a list of office files which have been found on the remote SMB
shares :

  + C$ :

    - C:\Windows\System32\MSDRM\MsoIrmProtector.doc
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.doc
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_973a2dbdbe834c5f\MsoIrmProtector.doc
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_a18ed80ff2e40e5a\MsoIrmProtector.doc
    - C:\Windows\System32\MSDRM\MsoIrmProtector.ppt
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_973a2dbdbe834c5f\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_a18ed80ff2e40e5a\MsoIrmProtector.ppt
    - C:\Windows\System32\MSDRM\MsoIrmProtector.xls
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.xls
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_973a2dbdbe834c5f\MsoIrmProtector.xls
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.20348.1_none_a18ed80ff2e40e5a\MsoIrmProtector.xls
```

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx

https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

Plugin Output

tcp/445/cifs

```
Share path : \\S-DC\NETLOGON
Local path : C:\Windows\SYSVOL\sysvol\swansea.acca\SCRIPTS
Comment : Logon server share
[*] Allow ACE for Everyone (S-1-1-0): 0x001200a9
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        NO
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for BUILTIN\Administrators (S-1-5-32-544): 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\S-DC\SYSVOL
Local path : C:\Windows\SYSVOL\sysvol
Comment : Logon server share
[*] Allow ACE for Everyone (S-1-1-0): 0x001200a9
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        NO
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for BUILTIN\Administrators (S-1-5-32-544): 0x001f01ff
    FILE_GENERIC_READ:         YES
```

```
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for NT AUTHORITY\Authenticated Users (S-1-5-11): 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\S-DC\VShare
Local path : C:\Shares\VShare
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following shares can be accessed as Administrator :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
ADFS
ADWS
appcompat
apppatch
AppReadiness
assembly
AzureArcSetup
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
BrowserCore
CbsTemp
Containers
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
DirectAccess
```

```
Downloaded Program Files
drivers
DtcInstall.log
ELAMBKUP
en-US
explorer.exe
Fonts
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
iis.log
IME
ImmersiveControlPanel
INF
InputMethod
Installer
L2Schemas
LiveKernelReports
Logs
lsasetup.log
Media
MEMORY.DMP
mib.bin
Microsoft.NET
Migration
Minidump
ModemLogs
notepad.exe
NTDS
OCR
Offline Web Pages
Panther
Performance
PFRO.log
PLA
PolicyDefinitions
Prefetch
PrintDialog
Provisioning
rdcbDb
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServerDataCenter.xml
ServiceProfiles
ServiceState
servicing
Setup
setupact.log
setuperr.log
ShellComponents
ShellExperiences
SKB
smtpins.log
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
SystemResources
```

```
SystemTemp
SYSVOL

- VShare  - (readable,writable)
  + Content of this share :
..
New folder
test.txt

- SYSVOL  - (readable,writable)
  + Content of this share :
..
swansea.acca

- NETLOGON  - (readable,writable)
  + Content of this share :
..

- C$  - (readable,writable)
  + Content of this share :
Documents and Settings
DumpStack.log
DumpStack.log.tmp
FTPRoot
inetpub
new_important_file.txt
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
Shares
StorageReports
System Volume Information
Users
Windows
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host when logged in as Administrator:

  - ADMIN$
  - C$
  - IPC$
  - NETLOGON
  - SYSVOL
  - VShare
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.1        Windows 10
```

92368 - Microsoft Windows Scripting Host Settings

Synopsis

Nessus was able to collect and report the Windows scripting host settings from the remote host.

Description

Nessus was able to collect system and user level Windows scripting host settings from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/23

Plugin Output

tcp/0

```
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\activedebugging : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\activedebugging : 1

Windows scripting host configuration attached.
```

200493 - Microsoft Windows Start Menu Software Version Enumeration

Synopsis

Enumerates Start Menu software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.

Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
The following software information is available on the remote host :

 - Azure Arc Setup.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Azure Arc Setup.lnk
     Target       : C:\Windows\AzureArcSetup\ArcSetup\AzureArcSetup.exe
     Version      : 1.0.0.0

 - Google Chrome.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Google Chrome.lnk
     Target       : C:\Program Files\Google\Chrome\Application\chrome.exe
     Version      : 143.0.7499.170

 - Immersive Control Panel.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Immersive Control
 Panel.lnk
     Target       : C:\Windows\System32\Control.exe
     Version      : 10.0.20348.2849

 - Microsoft Edge.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Microsoft Edge.lnk
     Target       : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
     Version      : 143.0.3650.96
```

```
- Server Manager.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Server Manager.lnk
    Target       : C:\Windows\system32\ServerManager.exe
    Version      : 10.0.20348.1

- Speech Recognition.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessibility\Speech
Recognition.lnk
    Target       : C:\Windows\Speech\Common\sapisvr.exe
    Version      : 5.3.25707.0

- Calculator.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Calculator.lnk
    Target       : C:\Windows\system32\win32calc.exe
    Version      : 10.0.20348.2849

- Math Input Panel.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Math Input
Panel.lnk
    Target       : C:\Program Files\Common Files\Microsoft Shared\Ink\mip.exe
    Version      : 10.0.20348.2849

- Notepad.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Notepad.lnk
    Target       : C:\Windows\system32\notepad.exe
    Version      : 10.0.2034 [...]
```

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi on\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2012/03/23, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
The following startup item was found :

  AzureArcSetup - %windir%\AzureArcSetup\Systray\AzureArcSysTray.exe
  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
```

38153 - Microsoft Windows Summary of Missing Patches

Synopsis

The remote host is missing several Microsoft security patches.

Description

This plugin summarizes updates for Microsoft Security Bulletins or Knowledge Base (KB) security updates that have not been installed on the remote Windows host based on the results of either a credentialed check using the supplied credentials or a check done using a supported third-party patch management tool.

Note the results of missing patches also include superseded patches.

Review the summary and apply any missing updates in order to be up to date.

Solution

Run Windows Update on the remote host or use a patch management solution.

Risk Factor

None

Plugin Information

Published: 2009/04/24, Modified: 2019/06/13

Plugin Output

tcp/445/cifs

```
The patches for the following bulletins or KBs are missing on the remote host :

  - KB5065306 ( https://support.microsoft.com/en-us/help/5065306 )
  - KB5065432 ( https://support.microsoft.com/en-us/help/5065432 )
  - KB5066782 ( https://support.microsoft.com/en-us/help/5066782 )
  - KB5068787 ( https://support.microsoft.com/en-us/help/5068787 )
```

92369 - Microsoft Windows Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2023/06/06

Plugin Output

tcp/0

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : GMT Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-262
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-261
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DynamicDaylightTimeDisabled : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightBias : 0xFFFFFFC4
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\Bias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000300050001000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000a0005000200000000000000000
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.11.1
Nessus build : 20021
Plugin feed version : 202512091520
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : S-DC Full Port Scan
```

```
Scan policy used : S-DC Host Discorvery Scan  -
Scanner IP : 192.168.1.2
Port scanner(s) : wmi_netstat
Port range : default
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'SWANSEA\Administrator' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/1/8 16:49 EST (UTC -05:00)
Scan duration : 3067 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

https://www.tenable.com/products/nessus/nessus-professional

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2025/11/03

Plugin Output

tcp/8834/www

```
URL     : https://192.168.1.1:8834/
Version : unknown
```

43815 - NetBIOS Multiple IP Address Enumeration

Synopsis

The remote host is configured with multiple IP addresses.

Description

By sending a special NetBIOS query, Nessus was able to detect the use of multiple IP addresses on the remote host. This indicates the host may be running virtualization software, a VPN client, or has multiple network interfaces.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/06, Modified: 2011/09/02

Plugin Output

udp/137/netbios-ns

```
The remote host appears to be using the following IP addresses :

  - 10.0.2.15
  - 192.168.1.1
  - 20.0.0.1
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/0

```
Note that 2502 UDP ports belonging to DNS.exe have been ignored.
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/7/echo

```
Port 7/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/7

```
Port 7/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/9/discard

```
Port 9/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/9

```
Port 9/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/13/daytime

```
Port 13/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/13/daytime

```
Port 13/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/17/qotd

```
Port 17/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/17/qotd

```
Port 17/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/19/chargen

```
Port 19/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/19

```
Port 19/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/53/dns

```
Port 53/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/67

```
Port 67/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/88

```
Port 88/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/88

```
Port 88/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/123/ntp

```
Port 123/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/137/netbios-ns

```
Port 137/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/161

```
Port 161/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/389/ldap

```
Port 389/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/389

```
Port 389/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/464

```
Port 464/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/464

```
Port 464/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/515

```
Port 515/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/593/http-rpc-epmap

```
Port 593/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/636

```
Port 636/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/1645

```
Port 1645/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/1646

```
Port 1646/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/1812

```
Port 1812/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/1813

```
Port 1813/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/2535

```
Port 2535/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/3268/ldap

```
Port 3268/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/3269

```
Port 3269/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/3388/ncacn_http

```
Port 3388/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/3391

```
Port 3391/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/3702

```
Port 3702/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/5355/llmnr

```
Port 5355/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/5357/www

```
Port 5357/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/5504/dce-rpc

```
Port 5504/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/5985/www

```
Port 5985/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/9389

```
Port 9389/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/47001/www

```
Port 47001/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/49664/dce-rpc

```
Port 49664/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/49665/dce-rpc

```
Port 49665/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/49666/dce-rpc

```
Port 49666/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/49667/dce-rpc

```
Port 49667/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/49668/dce-rpc

```
Port 49668/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/54401/dce-rpc

```
Port 54401/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

udp/56422

```
Port 56422/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/59349/dce-rpc

```
Port 59349/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64492/ncacn_http

```
Port 64492/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64493/dce-rpc

```
Port 64493/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64499/dce-rpc

```
Port 64499/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64509/dce-rpc

```
Port 64509/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64539/dce-rpc

```
Port 64539/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64558/dce-rpc

```
Port 64558/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64559/dce-rpc

```
Port 64559/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/12/08

Plugin Output

tcp/64639/dce-rpc

```
Port 64639/tcp was found to be open
```

24272 - Network Interfaces Enumeration (WMI)

Synopsis

Nessus was able to obtain the list of network interfaces on the remote host.

Description

Nessus was able, via WMI queries, to extract a list of network interfaces on the remote host and the IP addresses attached to them.

Note that this plugin only enumerates IPv6 addresses for systems running Windows Vista or later.

See Also

http://www.nessus.org/u?b362cab2

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/03, Modified: 2025/12/08

Plugin Output

tcp/0

```
+ Network Interface Information :

 - Network Interface = [00000001] Intel(R) PRO/1000 MT Desktop Adapter
 - MAC Address = 08:00:27:1A:80:9D
 - IPAddress/IPSubnet = 10.0.2.15/255.255.255.0
 - IPAddress/IPSubnet = fe80::e147:b674:a231:8284/64
 - IPAddress/IPSubnet = fd17:625c:f037:2:cfd0:7c37:27cc:3d7/64

+ Network Interface Information :

 - Network Interface = [00000002] Intel(R) PRO/1000 MT Desktop Adapter
 - MAC Address = 08:00:27:2A:B5:B6
 - IPAddress/IPSubnet = 192.168.1.1/255.255.255.0
 - IPAddress/IPSubnet = fe80::3e44:49fe:e3f3:83e6/64

+ Network Interface Information :

 - Network Interface = [00000003] Intel(R) PRO/1000 MT Desktop Adapter
 - MAC Address = 08:00:27:99:DA:4A
 - IPAddress/IPSubnet = 20.0.0.1/255.255.255.252
 - IPAddress/IPSubnet = fe80::3183:de30:e5e8:b7d0/64
```

```
+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    0.0.0.0         0.0.0.0         10.0.2.2
    10.0.2.0        255.255.255.0   0.0.0.0
    10.0.2.15       255.255.255.255 0.0.0.0
    10.0.2.255      255.255.255.255 0.0.0.0
    20.0.0.0        255.255.255.252 0.0.0.0
    20.0.0.1        255.255.255.255 0.0.0.0
    20.0.0.3        255.255.255.255 0.0.0.0
    127.0.0.0       255.0.0.0       0.0.0.0
    127.0.0.1       255.255.255.255 0.0.0.0
    127.255.255.255 255.255.255.255 0.0.0.0
    192.168.1.0     255.255.255.0   0.0.0.0
    192.168.1.1     255.255.255.255 0.0.0.0
    192.168.1.255   255.255.255.255 0.0.0.0
    192.168.2.0     255.255.255.0   20.0.0.2
    224.0.0.0       240.0.0.0       0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.

No sensitive information has been disclosed.

Version : unknown
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Microsoft Windows Server 2022
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Microsoft Windows Server 2022 Datacenter 20348
Confidence level : 80
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 100
Method : SMB_OS
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 50
Method : FTP
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 70
```

```
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B11113:F0x12:W65392:O0204ffff:M1460:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=9

Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 70
Method : HTTP
Type : general-purpose
Fingerprint : HTTP:Server: Microsoft-HTTPAPI/2.0


Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 70
Method : smb
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 NTP:!:unknown
SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:S-DCs/O:Nessus Users Uniteds/OU:Nessus Server
6d151ccc77fc0cda95013aa8c90e9a730518458d
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2022 Datacenter Build 20348
Confidence level : 100
Method : SMB_OS

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

NTP:!:unknown
SinFP:
   P1:B11113:F0x12:W65392:O0204ffff:M1460:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=9
HTTP:Server: Microsoft-HTTPAPI/2.0

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:S-DCs/O:Nessus Users Uniteds/OU:Nessus Server
6d151ccc77fc0cda95013aa8c90e9a730518458d



The remote host is running Microsoft Windows Server 2022 Datacenter Build 20348
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/445/cifs

```
OS Security Patch Assessment is available.

Account  : SWANSEA\Administrator
Protocol : SMB
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 3269 was detected as being open but is now closed
Port 64559 was detected as being open but is now closed
```

92426 - OpenSaveMRU History

Synopsis

Nessus was able to enumerate opened and saved files on the remote host.

Description

Nessus was able to generate a report on files that were opened using the shell dialog box or saved using the shell dialog box. This is the box that appears when you attempt to save a document or open a document in Windows Explorer.

See Also

http://www.nessus.org/u?ac4dd3fb

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/23

Plugin Output

tcp/0

```
Open / Save report attached.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/11/11

Plugin Output

tcp/0

```
. You need to take the following 2 actions :

+ Install the following Microsoft patches :
- KB5068787 (4 vulnerabilities)
- KB5065306 (1 vulnerabilities)
```

92428 - Recent File History

Synopsis

Nessus was able to enumerate recently opened files on the remote host.

Description

Nessus was able to gather evidence of files opened by file type from the remote host.

See Also

https://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
C:\\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\WorkingPSScripts.lnk

Recent files found in registry and appdata attached.
```

92429 - Recycle Bin Files

Synopsis

Nessus was able to enumerate files in the recycle bin on the remote host.

Description

Nessus was able to generate a list of all files found in $Recycle.Bin subdirectories.

See Also

http://www.nessus.org/u?0c1a03df

http://www.nessus.org/u?61293b38

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
C:\\$Recycle.Bin\\.
C:\\$Recycle.Bin\\..
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\.
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\..
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I00WHJ7.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I0J131S.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I14S639.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I3J4SKP.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I4LQ4U2.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I56UIK2.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I7JEYRG.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I998QH7.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$I9T0TZR.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IBQOQVF.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$ICEY7CT.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$ICU5AQZ.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$ICYKRK1.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IEKM3R3.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IET0BJA.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IEU85SX.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IFL44F4.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IG2EZ2S.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IGHCOUG.ps1
```

```
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IIOM1AI.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IJ7KC3J.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$IK0UY0P.ps1
C:\\$Recycle.Bin\\S-1-5-21-3861473089-3053040122-1338177554-500\$ILG4TEZ.txt
C:\\$Recycle.Bin\\S-1-5-21-3861473089-30 [...]
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.

However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/443/www

```
The target TLS server offers no post-quantum ciphers.
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.

However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/8834/www

```
The target TLS server offers no post-quantum ciphers.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
This port supports TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: S-DC

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 8C 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 27 18:00:38 2025 GMT
Not Valid After: Oct 26 18:00:38 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E6 E7 27 59 A3 2A E5 E8 00 9A 48 1E 51 35 3F 13 F9 C5 28
```

```
             6F 14 B2 7B A6 E2 85 C4 05 30 C1 03 5E FB 2A AF CC D1 42 03
             FD 8B 8B 98 EF 09 0C 6A EB 9C 66 A8 B7 BC 17 CA 3E 10 8F C4
             1D C7 B7 DF FB 56 26 41 2C BA FC B1 E5 76 59 84 8F 75 DD 3C
             34 4B 27 57 53 11 CC DB 06 03 95 A7 F8 68 27 B2 F1 2F 5B 61
             B3 9C D2 BC B7 DB 59 43 20 13 DC 0D AD 1F 05 E6 2E AD 28 C5
             5A 56 48 DC 9A 51 05 3B 0D FB E6 64 77 B5 43 1B 13 1C 0D F1
             CD 30 80 AE FA C5 54 2F D9 13 B1 57 EE A7 FE C2 A3 63 B1 F9
             3B 5B 65 88 E0 67 BC 14 06 31 45 FE 7D 9A AB 81 12 A6 48 09
             DE C7 2B 41 76 EA F3 E9 45 D6 0A A0 FB E6 04 AF 86 F7 4E 8F
             68 83 F0 9E 21 7E 08 14 01 38 34 94 32 B0 AF EF 80 31 BA 67
             72 C1 15 53 55 2C 76 76 9B F6 2F F0 7A 44 83 D7 16 28 AA 25
             A5 83 F3 81 CC AC 8E E0 5F 80 71 A4 68 1B CA FC 67
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 76 AD 8A 42 BF B8 2C DC 89 E0 0B 8E F9 A5 24 BA 5F D7 BA
           68 A4 96 B0 A6 29 D6 60 66 03 76 F0 DC 7C B2 AD CA 3D 68 E9
           8E DB 50 E1 BC CC A0 9E 94 FC 82 EC 05 D6 AF 3C 6C 19 F9 CD
           C5 17 04 91 6F 98 BC 63 6E 10 55 EF 32 81 59 5E 3E 4D 00 DE
           56 4D 60 F4 01 1A 99 93 CF AE B2 FC 10 61 26 75 4C 47 BF DB
           E9 EC 7C 1F 95 15 F5 59 D7 8E D5 BF 08 7B 3F 48 19 7A 51 F9
           86 96 77 BA 57 78  [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDHE         RSA      AES-CBC(256)
 SHA1
```

```
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 SHA384


SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
```

```
   ----------------------        ----------      ---          ----     --------------------  ---
   DHE-RSA-AES128-SHA256         0x00, 0x9E      DHE          RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DHE          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDHE        RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDHE        RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C      RSA          RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D      RSA          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDHE        RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDHE        RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F      RSA          RSA      AES-CBC(128)
SHA1
   AE [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8834/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 SHA384


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDHE         RSA      AES-GCM(256)
 SHA384

The fields above are :
```

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DHE           RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DHE           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDHE         RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDHE         RSA      AES-CBC(128)
 SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8834/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDHE         RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DHE           RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DHE           RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D        RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDHE         RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDHE         RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange} [...]
```

97086 - Server Message Block (SMB) Protocol Version 1 Enabled

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

Plugin Information

Published: 2017/02/09, Modified: 2020/06/12

Plugin Output

tcp/445/cifs

```
SMBv1 server is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : NULL or missing
SMB1protocol feature is enabled based on the following key :
  - HKLM\SYSTEM\CurrentControlSet\Services\srv
SMBv1 client is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10\Start : 2
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote host supports the SMBv1 protocol.

Description

The remote host (Windows and/or Samba server) supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, most security and compliance agencies recommend that users disable SMBv1 per SMB best practices.

See Also

http://www.nessus.org/u?59bfc3ef

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2025/08/13

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

160486 - Server Message Block (SMB) Protocol Version Detection

Synopsis

Verify the version of SMB on the remote host.

Description

The Server Message Block (SMB) Protocol provides shared access to files and printers across nodes on a network.

See Also

http://www.nessus.org/u?f463096b

http://www.nessus.org/u?1a4b3744

Solution

Disable SMB version 1 and block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Risk Factor

None

Plugin Information

Published: 2022/05/04, Modified: 2022/05/04

Plugin Output

tcp/445/cifs

```
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB2 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB3 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : Key not found.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/7/echo

```
An echo server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/19/chargen

```
A chargen server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/443/www

```
A TLSv1.3 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.3.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/593/http-rpc-epmap

```
An http-rpc-epmap is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/3388/ncacn_http

```
An ncacn_http server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/5357/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/5985/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/8834/www

```
A TLSv1.3 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.3.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/47001/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2025/12/08

Plugin Output

tcp/64492/ncacn_http

```
An ncacn_http server is running on this port.
```

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/17/qotd

```
qotd seems to be running on this port.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/13/daytime

```
Daytime is running on this port.
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :

Strict-Transport-Security: max-age=31536000; includeSubDomains
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
h2
```

277654 - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/443/www

```
These are the TLS supported groups offered by the remote server :


TLS supported groups :

Name                 Code
---------------------------
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
secp384r1            0x0018
```

```
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1           0x0018
secp384r1     [...]
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/443/www

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but there were intermittent authentication failures.

Description

Nessus was able to successfully authenticate to the remote host on an authentication protocol at least once using credentials provided in the scan policy.

However, one or more plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that was previously successful. This may indicate an intermittent authentication problem with the remote host, which could be caused by session rate limits, session concurrency limits, or other issues preventing consistent authentication success.

These intermittent authentication failures may have affected the results of some plugins. See plugin output for failure details.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2018/10/02, Modified: 2024/03/25

Plugin Output

tcp/445/cifs

```
Nessus was able to successfully log into the remote host as :

User:       'SWANSEA\Administrator'
Port:       445
Proto:      SMB
Method:     password


Successful authentication was reported by the following plugin :

  Plugin      : smb_login.nasl
```

```
  Plugin ID   : 10394
  Plugin Name : Microsoft Windows SMB Log In Possible

However, one or more subsequent plugins failed to authenticate to the
remote host on the same port and protocol using the same credential
set that previously succeeded. This may indicate an intermittent
authentication problem with the remote host which may have affected
the results of the following plugins.

Error message statistics :

  33 Failed to open a socket on port 445. This failure may have prevented
     a login attempt. The failure references the previously successful
     login account for tracking purposes.


Failure Details :

  - Plugin      : windows_autoruns_internet_explorer.nbin
    Plugin ID   : 70619
    Plugin Name : Microsoft Windows AutoRuns Internet Explorer
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : windows_autoruns_image_HiJacks.nbin
    Plugin ID   : 70618
    Plugin Name : Microsoft Windows AutoRuns Registry Hijack Possible Locations
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : windows_autoruns_explorer.nbin
    Plugin ID   : 70617
    Plugin Name : Microsoft Windows AutoRuns Explorer
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : windows_autoruns_appInit_dll.nbin
    Plugin ID   : 70614
    Plugin Name : Microsoft Windows AutoRuns Appinit DLLs
    Message     :
Failed to op [...]
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/445/cifs

```
Nessus was able to log in to the remote host via the following :

User:       'SWANSEA\Administrator'
Port:       445
Proto:      SMB
Method:     password
```

165454 - Tenable Nessus Installed (Windows)

Synopsis

Tenable Nessus is installed on the remote Windows host.

Description

Tenable Nessus is installed on the remote Windows host.

See Also

https://www.tenable.com/products/nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/09/26, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
Path           : C:\Program Files\Tenable\Nessus\
Version        : 10.10.0
Build          : 20152
Version Source : C:\ProgramData\Tenable\Nessus\nessus\nessus.version
```

161691 - The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)

Synopsis

Checks for the HKEY_CLASSES_ROOT\ms-msdt registry key.

Description

The remote host has the HKEY_CLASSES_ROOT\ms-msdt registry key. This is a known exposure for CVE-2022-30190.

Note that Nessus has not tested for CVE-2022-30190. It is only checking if the registry key exists. The recommendation is to apply the latest patch.

See Also

http://www.nessus.org/u?440e4ba1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

http://www.nessus.org/u?b9345997

Solution

Apply the latest Cumulative Update.

Risk Factor

None

Plugin Information

Published: 2022/05/31, Modified: 2022/07/28

Plugin Output

tcp/445/cifs

```
The HKEY_CLASSES_ROOT\ms-msdt registry key exists on the target. This may indicate that the target
 is vulnerable to CVE-2022-30190, if the vendor patch is not applied.
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
20260108212555.500000+000
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.2 to 192.168.1.1 :
192.168.1.2
192.168.1.1

Hop Count: 1
```

92434 - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
C:\\Users\Administrator\Downloads\ChromeSetup.exe
C:\\Users\Administrator\Downloads\desktop.ini
C:\\Users\Administrator\Downloads\Files\accb6000.txt
C:\\Users\Administrator\Downloads\Nessus-10.10.0-x64.msi
C:\\Users\Administrator\Downloads\Target Lab Vulnerability Scan_2iyon5.html
C:\\Users\Administrator\Downloads\Wireshark-4.6.0-x64.exe
C:\\Users\Public\Downloads\desktop.ini

Download folder content report attached.
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
SWANSEA.ACCA\Administrator
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\Administrator\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\Administrator\AppData\Roaming\Microsoft
\Windows\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\Administrator\Downloads
  - recent : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\Administrator\Videos
  - my music : C:\Users\Administrator\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\Administrator\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\Administrator\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\Administrator\AppData\LocalLow
  - sendto : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\Administrator\Documents
  - administrative tools : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu
\Programs\Administrative Tools
  - startup : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\Administrator\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\Administrator\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\Administrator\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function instead
  - local appdata : C:\Users\Administrator\AppData\Local
  - my pictures : C:\Users\Administrator\Pictures
  - templates : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Use [...]
```

92435 - UserAssist Execution History

Synopsis

Nessus was able to enumerate program execution history on the remote host.

Description

Nessus was able to gather evidence from the UserAssist registry key that has a list of programs that have been executed.

See Also

https://www.nirsoft.net/utils/userassist_view.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2019/11/12

Plugin Output

tcp/0

```
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\file explorer.lnk
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\windows powershell\windows powershell.lnk
c:\users\administrator\desktop\microsoft edge.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\notepad.exe
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\system tools\command prompt.lnk
ueme_ctlsession
c:\users\administrator\downloads\chromesetup.exe
msedge
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\google chrome.lnk
microsoftwindows.client.cbs_cw5n1h2txyewy!screenclipping
microsoft.autogenerated.{bd3f924e-55fb-a1ba-9de6-b50f9f2460ac}
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\microsoft edge.lnk
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\system tools\control panel.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\cmd.exe
microsoft.windows.controlpanel
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\services.msc
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\systempropertiescomputername.exe
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\mspaint.exe
chrome.userdata.systemprofile
ueme_ctlcuacount:ctor
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\windowspowershell\v1.0\powershell_ise.exe
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\inetsrv\inetmgr.exe
```

```
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\snipping tool.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\servermanager.exe
microsoft.autogenerated.{10e44728-9143-c317-94d4-fe5a949ebc66}
microsoft.windows.shell.rundialog
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\credentialuibroker.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\notepad.lnk
microsoft.windows.windowsinstaller
microsoft.autogenerated.{9ad5a3a4-1821-c8f2-f6cd-500884b24b63}
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\shutdown.exe
{f38bf404-1d43-42f2-9305-67de0b28fc23}\systemtemp\google6472_1181835840\bin\updater.exe
chrome.userdata.profile1
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\windows powershell\windows powershell ise.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\snippingtool.exe
{ [...]
```

24269 - WMI Available

Synopsis

WMI queries can be made against the remote host.

Description

The supplied credentials can be used to make WMI (Windows Management Instrumentation) requests against the remote host over DCOM.

These requests can be used to gather information about the remote host, such as its current state, network interface configuration, etc.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/03, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
The remote host returned the following caption from Win32_OperatingSystem:

Microsoft Windows Server 2022 Datacenter
```

71637 - WMI IIS ISAPI Extension Enumeration

Synopsis

The remote host has ISAPI extensions set up with IIS.

Description

The remote host is running one or more ISAPI IIS extensions such as ASP.NET installed. This plugin enumerates these extensions by examining the ISAPI filters and displays information on whether the extension is enabled or disabled.

See Also

http://www.iis.net/configreference/system.webserver/isapifilters

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/12/20, Modified: 2025/12/08

Plugin Output

tcp/0

```
IIS component  : Active Server Pages
Component path : C:\Windows\system32\inetsrv\asp.dll
Enabled ?      : Yes

IIS component  : Internet Printing
Component path : C:\Windows\system32\msw3prt.dll
Enabled ?      : Yes

IIS component  : ASP.NET v4.0.30319
Component path : C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
Enabled ?      : Yes

IIS component  : ASP.NET v2.0.50727
Component path : C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_isapi.dll
Enabled ?      : Yes

IIS component  : ASP.NET v4.0.30319
Component path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll
Enabled ?      : Yes

IIS component  : RPC Proxy Server Extension
Component path : %windir%\System32\RpcProxy\RpcProxy.dll
```

```
    Enabled ?       : Yes
```

52001 - WMI QuickFixEngineering (QFE) Enumeration

Synopsis

The remote Windows host has quick-fix engineering updates installed.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via WMI.

See Also

http://www.nessus.org/u?0c4ec249

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/16, Modified: 2025/12/08

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB5049617
  - Description : Update
  - InstalledOn : 8/8/2025

+ KB5063880
  - Description : Security Update
  - InstalledOn : 8/8/2025

+ KB5062793
  - Description : Security Update
  - InstalledOn : 8/8/2025

Note that for detailed information on installed QFE's such as InstalledBy, Caption,
and so on, please run the scan with 'Report Verbosity' set to 'verbose'.
```

44871 - WMI Windows Feature Enumeration

Synopsis

It is possible to enumerate Windows features using WMI.

Description

Nessus was able to enumerate the server features of the remote host by querying the 'Win32_ServerFeature' class of the '\Root\cimv2' WMI namespace for Windows Server versions or the 'Win32_OptionalFeature' class of the '\Root\cimv2' WMI namespace for Windows Desktop versions.

Note that Features can only be enumerated for Windows 7 and later for desktop versions.

See Also

https://msdn.microsoft.com/en-us/library/cc280268

https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/querying-the-status-of-optional-features

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0754

Plugin Information

Published: 2010/02/24, Modified: 2025/12/08

Plugin Output

tcp/0

```
Nessus enumerated the following Windows features :

  - .NET Extensibility 4.8
  - .NET Framework 4.8
  - .NET Framework 4.8 Features
  - AD DS Snap-Ins and Command-Line Tools
  - AD DS Tools
  - AD DS and AD LDS Tools
  - ASP
  - ASP.NET 4.8
  - ASP.NET 4.8
  - Active Directory Administrative Center
```

```
- Active Directory Domain Services
- Active Directory module for Windows PowerShell
- Application Development
- Azure Arc Setup
- Basic Authentication
- Client Certificate Mapping Authentication
- Common HTTP Features
- DHCP Server
- DHCP Server Tools
- DNS Server
- DNS Server Tools
- Default Document
- Deployment Server
- DirectAccess and VPN (RAS)
- Directory Browsing
- FTP Server
- FTP Service
- Feature Administration Tools
- File Server
- File Server Resource Manager
- File Server Resource Manager Tools
- File Server VSS Agent Service
- File Services Tools
- File and Storage Services
- File and iSCSI Services
- Group Policy Management
- HTTP Errors
- HTTP Logging
- HTTP Redirection
- Health and Diagnostics
- IIS 6 Management Compatibility
- IIS 6 Management Console
- IIS 6 Metabase Compatibility
- IIS Hostable Web Core
- IIS Management Console
- IIS Management Scripts and Tools
- IP and Domain Restrictions
- ISAPI Extensions
- ISAPI Filters
- Internet Printing
- LPD Service
- Logging Tools
- Management Tools
- Microsoft Defender Antivirus
- Network Policy and Access Services
- Network Policy and Access Services Tools
- ODBC Logging
- Performance
- Print Server
- Print and Document Services
- Print and Document Services Tools
- RAS Connection Manager Administration Kit (CMAK)
- RPC over HTTP Proxy
- Remote Access
- Remote Access GUI and Command-Line Tools
- Remote Access Management Tools
- Remote Access module for Windows PowerShell
- Remote Desktop Connection Broker
- Remote Desktop Gateway
- Remote Desktop Gateway Tools
- Remote Desktop Services
- Remote Desktop Services Tools
- Remote De [...]
```

33139 - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man

https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985/www

```
Here is some information about the WS-Management Server :

  Product Vendor  : Microsoft Corporation
  Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

162174 - Windows Always Installed Elevated Status

Synopsis

Windows AlwaysInstallElevated policy status was found on the remote Windows host

Description

Windows AlwaysInstallElevated policy status was found on the remote Windows host.

You can use the AlwaysInstallElevated policy to install a Windows Installer package with elevated (system) privileges This option is equivalent to granting full administrative rights, which can pose a massive security risk. Microsoft strongly discourages the use of this setting.

Solution

If enabled, disable AlwaysInstallElevated policy per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/06/14, Modified: 2022/06/14

Plugin Output

tcp/445/cifs

```
AlwaysInstallElevated policy is not enabled under HKEY_LOCAL_MACHINE.
AlwaysInstallElevated policy is not enabled under HKEY_USERS
 user:S-1-5-21-3861473089-3053040122-1338177554-500
```

48337 - Windows ComputerSystemProduct Enumeration (WMI)

Synopsis

It is possible to obtain product information from the remote host using WMI.

Description

By querying the WMI class 'Win32_ComputerSystemProduct', it is possible to extract product information about the computer system such as UUID, IdentifyingNumber, vendor, etc.

See Also

http://www.nessus.org/u?a21ce849

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/16, Modified: 2025/12/08

Plugin Output

tcp/0

```
+ Computer System Product
  - IdentifyingNumber : VirtualBox-dff36028-f2df-4c42-a41b-ed49d57e2617
  - Description       : Computer System Product
  - Vendor            : innotek GmbH
  - Name              : VirtualBox
  - UUID              : DFF36028-F2DF-4C42-A41B-ED49D57E2617
  - Version           : 1.2
```

159817 - Windows Credential Guard Status

Synopsis

Retrieves the status of Windows Credential Guard.

Description

Retrieves the status of Windows Credential Guard.

Credential Guard prevents attacks such as such as Pass-the-Hash or Pass-The-Ticket by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

See Also

http://www.nessus.org/u?fb8c8c37

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/04/18, Modified: 2023/08/25

Plugin Output

tcp/445/cifs

```
Windows Credential Guard is not fully enabled.
The following registry keys have not been set :
  - System\CurrentControlSet\Control\DeviceGuard\RequirePlatformSecurityFeatures : Key not found.
  - System\CurrentControlSet\Control\LSA\LsaCfgFlags : Key not found.
  - System\CurrentControlSet\Control\DeviceGuard\EnableVirtualizationBasedSecurity : Key not found.
```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/03/01, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {699a637d-5358-4e9d-9d93-6305944127c3}
Network Connection : Internet
DhcpNameServer: 192.168.1.1

Interface: {e6f785e0-7f95-4fab-8156-b32b4ca39791}
Network Connection : External
NameServer: 127.0.0.1

Interface: {db6d5f66-996d-4af3-a947-3c7aede6b72d}
Network Connection : IntSwa
NameServer: 127.0.0.1

Interface: Default
DhcpNameServer: 192.168.1.1
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

https://www.microsoft.com/en-us/windows/comprehensive-security

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/15, Modified: 2025/12/08

Plugin Output

tcp/0

```
Path                          : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25110.6-0\
Version                       : 4.18.25110.6
Engine Version                : 1.1.25110.1
Malware Signature Timestamp : Jan.  8, 2026 at 11:51:35 GMT
Malware Signature Version   : 1.443.564.0
Security Agent Identifier   : A934B2D9-8D49-B8DD-A12E-F5E5DD6658AE
Signatures Last Updated     : Jan.  8, 2026 at 21:38:27 GMT
```

72482 - Windows Display Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the display drivers on the remote host.

Description

Nessus was able to enumerate one or more of the display drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?b6e87533

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0756

Plugin Information

Published: 2014/02/06, Modified: 2025/12/08

Plugin Output

tcp/0

```
Device Name         : Microsoft Basic Display Adapter
Driver File Version : 10.0.20348.1
Driver Date         : 06/21/2006
Video Processor     : VirtualBox VESA BIOS
```

171956 - Windows Enumerate Accounts

Synopsis

Enumerate Windows accounts.

Description

Enumerate Windows accounts.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/28, Modified: 2025/12/08

Plugin Output

tcp/0

```
Windows accounts enumerated. Results output to DB.
User data gathered in scan starting at : 2026/1/8 16:49 EST
```

92423 - Windows Explorer Recently Executed Programs

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to find evidence of program execution using Windows Explorer registry logs and settings.

See Also

http://www.forensicswiki.org/wiki/LastVisitedMRU

http://www.nessus.org/u?7e00b191

http://www.nessus.org/u?ac4dd3fb

http://www.nessus.org/u?c409cb41

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2019/08/15

Plugin Output

tcp/0

```
msedge.exePO :i+00.9#K&]B_
PowerShell_ISE.exePO :i+00:.9#K&]B_&&Nad-..
notepad.exePO :i+00.9#K&]B_
cmd\1
adbec
\\ACCB6000\1
services.msc\1
dnsmgmt.msc\1
ncpa.cpl\1
msedge.exeHq
PowerShell_ISE.exeq
NOTEPAD.EXEI]|O
PickerHost.exe,

 MRU programs details in attached report.
```

159929 - Windows LSA Protection Status

Synopsis

Windows LSA Protection is disabled on the remote Windows host.

Description

The LSA Protection validates users for local and remote sign-ins and enforces local security policies to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protects against Pass-the-Hash or Mimikatz-style attacks.

Solution

Enable LSA Protection per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/04/20, Modified: 2025/06/16

Plugin Output

tcp/445/cifs

```
LSA Protection Key \SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL not found.
```

148541 - Windows Language Settings Detection

Synopsis

This plugin enumerates language files on a windows host.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates language IDs listed on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/14, Modified: 2022/02/01

Plugin Output

tcp/0

```
Default Install Language Code: 1033

Default Active Language Code: 1033

Other common microsoft Language packs may be scanned as well.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 8 NetBIOS names have been gathered :

 S-DC             = Computer name
 SWANSEA          = Workgroup / Domain name
 SWANSEA          = Domain Controllers
 S-DC             = File Server Service
 SWANSEA          = Browser Service Elections
 SWANSEA          = Domain Master Browser
 SWANSEA          = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   08:00:27:2a:b5:b6
```

155963 - Windows Printer Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the printer drivers on the remote host.

Description

Nessus was able to enumerate one or more of the printer drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?fab99415

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/12/09, Modified: 2025/12/08

Plugin Output

tcp/445/cifs

```
--- Microsoft enhanced Point and Print compatibility driver ---

Nessus detected 2 installs of Microsoft enhanced Point and Print compatibility driver:

  Path               : C:\Windows\system32\spool\DRIVERS\x64\3\mxdwdrv.dll
  Version            : 10.0.20348.4050
  Supported Platform : Windows x64

  Path               : C:\Windows\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.20348.4050
  Supported Platform : Windows NT x86

--- Microsoft Print To PDF ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_0a3468baaae9fedd\Amd64\mxdwdrv.dll
  Version            : 10.0.20348.1
  Supported Platform : Windows x64

--- Microsoft XPS Document Writer v4 ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_0a3468baaae9fedd\Amd64\mxdwdrv.dll
  Version            : 10.0.20348.1
```

```
    Supported Platform : Windows x64
```

63620 - Windows Product Key Retrieval

Synopsis

This plugin retrieves the Windows Product key of the remote Windows host.

Description

Using the supplied credentials, Nessus was able to obtain the retrieve the Windows host's partial product key'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/01/18, Modified: 2013/01/18

Plugin Output

tcp/445/cifs

```
  Product key : XXXXX-XXXXX-XXXXX-XXXXX-33Y34

Note that all but the final portion of the key has been obfuscated.
```

160576 - Windows Services Registry ACL

Synopsis

Checks Windows Registry for Service ACLs

Description

Checks Windows Registry for Service ACLs.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2022/05/05, Modified: 2024/01/15

Plugin Output

tcp/445/cifs

```
Verbosity must be set to 'Report as much information as possible' for this plugin to produce output.
```

85736 - Windows Store Application Enumeration

Synopsis

It is possible to obtain the list of applications installed from the Windows Store.

Description

This plugin connects to the remote Windows host with the supplied credentials and uses WMI and Powershell to enumerate applications installed on the host from the Windows Store.

See Also

https://www.microsoft.com/en-us/store/apps

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/09/02, Modified: 2025/12/08

Plugin Output

tcp/0

```
  -1527c705-839a-4832-9118-54d4Bd6a0c89
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FilePicker_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -c5e2524a-ea46-4f67-841f-6a9465d9d515
      Version : 10.0.20348.1
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FileExplorer_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -E2A4F912-2574-4A75-9BB0-0D023378592B
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.AppResolverUX_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE
      Version : 10.0.20348.1
      InstallLocation : C:\Windows\SystemApps
\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_cw5n1h2txyewy
      Architecture : Neutral
```

```
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AAD.BrokerPlugin
    Version : 1000.19580.1000.0
    InstallLocation : C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
    Architecture : Neutral
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AccountsControl
    Version : 10.0.20348.1
    InstallLocation : C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy
    Architecture : Neutral
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AsyncTextService
    Version : 10.0.20348.1
    InstallLocation : C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe
    Architecture : Neutral
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.BioEnrollment
    Version : 10.0.19585.1001
 [...]
```

204960 - Windows System Driver Enumeration (Windows)

Synopsis

One or more kernel or file system drivers were enumerated on the remote Windows host.

Description

One or more kernel or file system drivers were enumerated on the remote Windows host.

See Also

http://www.nessus.org/u?43f8ab81

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/08/01, Modified: 2025/12/08

Plugin Output

tcp/0

```
Total : 356

  Name         : 1394ohci
  Path         : C:\Windows\system32\drivers\1394ohci.sys
  Service Type : Kernel Driver
  Description  : 1394 OHCI Compliant Host Controller
  State        : Stopped

  Name         : 3ware
  Path         : C:\Windows\system32\drivers\3ware.sys
  Service Type : Kernel Driver
  Description  : 3ware
  State        : Stopped

  Name         : ACPI
  Path         : C:\Windows\system32\drivers\ACPI.sys
  Service Type : Kernel Driver
  Description  : Microsoft ACPI Driver
  State        : Running

  Name         : AcpiDev
  Path         : C:\Windows\system32\drivers\AcpiDev.sys
  Service Type : Kernel Driver
  Description  : ACPI Devices driver
```

```
State        : Stopped

Name         : acpiex
Path         : C:\Windows\system32\Drivers\acpiex.sys
Service Type : Kernel Driver
Description  : Microsoft ACPIEx Driver
State        : Running

Name         : acpipagr
Path         : C:\Windows\system32\drivers\acpipagr.sys
Service Type : Kernel Driver
Description  : ACPI Processor Aggregator Driver
State        : Stopped

Name         : AcpiPmi
Path         : C:\Windows\system32\drivers\acpipmi.sys
Service Type : Kernel Driver
Description  : ACPI Power Meter Driver
State        : Stopped

Name         : acpitime
Path         : C:\Windows\system32\drivers\acpitime.sys
Service Type : Kernel Driver
Description  : ACPI Wake Alarm Driver
State        : Stopped

Name         : Acx01000
Path         : C:\Windows\system32\drivers\Acx01000.sys
Service Type : Kernel Driver
Description  : Acx01000
State        : Stopped

Name         : ADP80XX
Path         : C:\Windows\system32\drivers\ADP80XX.SYS
Service Type : Kernel Driver
Description  : ADP80XX
State        : Stopped

Name         : AFD
Path         : C:\Windows\system32\drivers\afd.sys
Service Type : Kernel Driver
Description  : Ancillary Function Driver for Winsock
State        : Running

Name         : afunix
Path         : C:\Windows\system32\drivers\afunix.sys
Servic [...]
```