Win2022_DavidStephens

Report generated by Nessus™ Wed, 21 Aug 2024 07:03:02 AEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.56.50

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	8	6	1	205

Scan Information

Start time: Wed Aug 21 06:49:08 2024
End time: Wed Aug 21 07:03:01 2024

Host Information

Netbios Name: DC
IP: 192.168.56.50
MAC Address: 08:00:27:AA:5F:7A 08:00:27:40:99:73
OS: Microsoft Windows Server 2022 Standard Build 20348

Vulnerabilities

202039 - KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5040437. It is, therefore, affected by multiple vulnerabilities

- RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. (CVE-2024-3596)

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/5040437

Solution

Apply Security Update 5040437

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

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

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

STIG Severity

I

References

CVE	CVE-2024-3596
CVE	CVE-2024-21417
CVE	CVE-2024-26184
CVE	CVE-2024-28899
CVE	CVE-2024-30013
CVE	CVE-2024-30071
CVE	CVE-2024-30079
CVE	CVE-2024-30081
CVE	CVE-2024-30098
CVE	CVE-2024-35270
CVE	CVE-2024-37969
CVE	CVE-2024-37970
CVE	CVE-2024-37971
CVE	CVE-2024-37972
CVE	CVE-2024-37973
CVE	CVE-2024-37974
CVE	CVE-2024-37975

CVE	CVE-2024-37977
CVE	CVE-2024-37981
CVE	CVE-2024-37984
CVE	CVE-2024-37986
CVE	CVE-2024-37987
CVE	CVE-2024-37988
CVE	CVE-2024-37989
CVE	CVE-2024-38010
CVE	CVE-2024-38011
CVE	CVE-2024-38013
CVE	CVE-2024-38015
CVE	CVE-2024-38017
CVE	CVE-2024-38019
CVE	CVE-2024-38022
CVE	CVE-2024-38025
CVE	CVE-2024-38027
CVE	CVE-2024-38028
CVE	CVE-2024-38030
CVE	CVE-2024-38031
CVE	CVE-2024-38033
CVE	CVE-2024-38034
CVE	CVE-2024-38041
CVE	CVE-2024-38043
CVE	CVE-2024-38044
CVE	CVE-2024-38047
CVE	CVE-2024-38048
CVE	CVE-2024-38049
CVE	CVE-2024-38050
CVE	CVE-2024-38051
CVE	CVE-2024-38052
CVE	CVE-2024-38053
CVE	CVE-2024-38054
CVE	CVE-2024-38055
CVE	CVE-2024-38056
CVE	CVE-2024-38057
CVE	CVE-2024-38058
CVE	CVE-2024-38059
CVE	CVE-2024-38060
CVE	CVE-2024-38061
CVE	CVE-2024-38062
CVE	CVE-2024-38064
CVE	CVE-2024-38065
CVE	CVE-2024-38067

CVE	CVE-2024-38068
CVE	CVE-2024-38069
CVE	CVE-2024-38070
CVE	CVE-2024-38071
CVE	CVE-2024-38072
CVE	CVE-2024-38073
CVE	CVE-2024-38074
CVE	CVE-2024-38076
CVE	CVE-2024-38077
CVE	CVE-2024-38079
CVE	CVE-2024-38080
CVE	CVE-2024-38085
CVE	CVE-2024-38091
CVE	CVE-2024-38099
CVE	CVE-2024-38100
CVE	CVE-2024-38101
CVE	CVE-2024-38102
CVE	CVE-2024-38104
CVE	CVE-2024-38105
CVE	CVE-2024-38112
CVE	CVE-2024-38517
CVE	CVE-2024-39684
MSKB	5040437
XREF	MSFT:MS24-5040437
XREF	CISA-KNOWN-EXPLOITED:2024/07/30
XREF	IAVA:2024-A-0408-S
XREF	IAVA:2024-A-0407-S

Plugin Information

Published: 2024/07/09, Modified: 2024/08/16

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5040437

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.20348.2520
    Should be      : 10.0.20348.2582
```

205456 - KB5041160: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (August 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5041160. It is, therefore, affected by multiple vulnerabilities

- An elevation of privilege vulnerability exists in Windows based systems supporting Virtualization Based Security (VBS) including a subset of Azure Virtual Machine SKUS. This can allow an attacker with administrator privileges to replace current versions of Windows system files with outdated versions. By exploiting this vulnerability, an attacker could reintroduce previously mitigated vulnerabilities, circumvent some features of VBS, and exfiltrate data protected by VBS. (CVE-2024-21302)

- A buffer overflow was found in grub_font_construct_glyph(). A malicious crafted pf2 font can lead to an overflow when calculating the max_glyph_size value, allocating a smaller than needed buffer for the glyph, this further leads to a buffer overflow and a heap based out-of-bounds write. An attacker may use this vulnerability to circumvent the secure boot mechanism. (CVE-2022-2601)

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/5041160

Solution

Apply Security Update 5041160

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.2

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-2022-2601
CVE	CVE-2022-3775
CVE	CVE-2023-40547
CVE	CVE-2024-21302
CVE	CVE-2024-29995
CVE	CVE-2024-37968
CVE	CVE-2024-38063
CVE	CVE-2024-38106
CVE	CVE-2024-38107
CVE	CVE-2024-38114
CVE	CVE-2024-38115
CVE	CVE-2024-38116
CVE	CVE-2024-38117
CVE	CVE-2024-38118
CVE	CVE-2024-38120
CVE	CVE-2024-38121
CVE	CVE-2024-38122
CVE	CVE-2024-38125
CVE	CVE-2024-38126
CVE	CVE-2024-38127
CVE	CVE-2024-38128
CVE	CVE-2024-38130
CVE	CVE-2024-38131
CVE	CVE-2024-38132
CVE	CVE-2024-38133
CVE	CVE-2024-38134
CVE	CVE-2024-38136
CVE	CVE-2024-38137
CVE	CVE-2024-38138
CVE	CVE-2024-38140
CVE	CVE-2024-38141
CVE	CVE-2024-38142
CVE	CVE-2024-38143

CVE	CVE-2024-38144
CVE	CVE-2024-38145
CVE	CVE-2024-38146
CVE	CVE-2024-38147
CVE	CVE-2024-38148
CVE	CVE-2024-38150
CVE	CVE-2024-38151
CVE	CVE-2024-38152
CVE	CVE-2024-38153
CVE	CVE-2024-38154
CVE	CVE-2024-38178
CVE	CVE-2024-38180
CVE	CVE-2024-38193
CVE	CVE-2024-38196
CVE	CVE-2024-38198
CVE	CVE-2024-38199
CVE	CVE-2024-38214
CVE	CVE-2024-38215
CVE	CVE-2024-38223
MSKB	5041160
XREF	MSFT:MS24-5041160
XREF	CISA-KNOWN-EXPLOITED:2024/09/03
XREF	IAVA:2024-A-0500
XREF	IAVA:2024-A-0499
XREF	IAVA:2024-A-0487

Plugin Information

Published: 2024/08/13, Modified: 2024/08/16

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5041160

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.20348.2520
    Should be      : 10.0.20348.2652
```

180360 - 7-Zip < 23.00 Multiple Vulnerabilities

Synopsis

A compression utility installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of 7-Zip installed on the remote Windows host is below 23.00. It is, therefore, affected by multiple vulnerabilities:

- A remote code execution vulnerability exists in 7-zip due to an integer underflow. An unauthenticated, remote attacker can exploit this, by tricking a user into opening a specially crafted archive, to execute arbitrary code on the system. (CVE-2023-31102)

- A remote code execution vulnerability exists in 7-zip due to an out-of-bounds write. An unauthenticated, remote attacker can exploit this, by tricking a user into opening a specially crafted archive, to execute arbitrary code on the system. (CVE-2023-40481)

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://www.7-zip.org/history.txt

https://www.zerodayinitiative.com/advisories/ZDI-23-1164/

Solution

Upgrade to 7-Zip version 23.00 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-31102
CVE	CVE-2023-40481
XREF	IAVA:2023-A-0440

Plugin Information

Published: 2023/08/31, Modified: 2023/11/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\7-Zip
Installed version : 22.1.0.0
Fixed version     : 23.00
```

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:  as vagrant/v******t

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

181867 - Notepad++ < 8.5.7 Multiple Buffer Overflow Vulnerabilities

Synopsis

The text editor on the remote Windows host is affected by multiple vulnerabilties.

Description

The version of Notepad++ installed on the remote host is prior to 8.5.7. It is, therefore, affected by multiple buffer overflow vulnerabilties. An authenticated, local attacker could exploit these to cause a denial of service condition or the execution of arbitrary code.

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

See Also

https://notepad-plus-plus.org/news/v857-released-fix-security-issues/

Solution

Upgrade to Notepad++ 8.5.7 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-40031
CVE	CVE-2023-40036
CVE	CVE-2023-40164
CVE	CVE-2023-40166

Plugin Information

Published: 2023/09/26, Modified: 2023/09/27

Plugin Output

tcp/0

```
Path              : C:\Program Files\Notepad++
Installed version : 8.5.3.0
Fixed version     : 8.5.7
```

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

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

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)

VPR Score

5.1

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: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
  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}
```

202304 - Security Updates for Microsoft .NET Framework (July 2024)

Synopsis

The Microsoft .NET Framework installation on the remote host is missing a security update.

Description

The Microsoft .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by remote code execution vulnerability.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38081
https://support.microsoft.com/en-us/help/5041017
https://support.microsoft.com/en-us/help/5041020
https://support.microsoft.com/en-us/help/5041016
https://support.microsoft.com/en-us/help/5041023
https://support.microsoft.com/en-us/help/5041022
https://support.microsoft.com/en-us/help/5041021
https://support.microsoft.com/en-us/help/5041026
https://support.microsoft.com/en-us/help/5039885
https://support.microsoft.com/en-us/help/5041024
https://support.microsoft.com/en-us/help/5041027
https://support.microsoft.com/en-us/help/5039895
https://support.microsoft.com/en-us/help/5041019
https://support.microsoft.com/en-us/help/5041018

Solution

Microsoft has released security updates for Microsoft .NET Framework.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-38081
MSKB	5041017
MSKB	5041020
MSKB	5041016
MSKB	5041023
MSKB	5041022
MSKB	5041021
MSKB	5041026
MSKB	5039885
MSKB	5041024
MSKB	5041027
MSKB	5039895
MSKB	5041019
MSKB	5041018
XREF	MSFT:MS24-5041017
XREF	MSFT:MS24-5041020
XREF	MSFT:MS24-5041016
XREF	MSFT:MS24-5041023
XREF	MSFT:MS24-5041022
XREF	MSFT:MS24-5041021
XREF	MSFT:MS24-5041026
XREF	MSFT:MS24-5039885
XREF	MSFT:MS24-5041024
XREF	MSFT:MS24-5041027
XREF	MSFT:MS24-5039895
XREF	MSFT:MS24-5041019
XREF	MSFT:MS24-5041018

XREF IAVA:2024-A-0399

Plugin Information

Published: 2024/07/12, Modified: 2024/07/15

Plugin Output

tcp/445/cifs

```
Microsoft .NET Framework 4.8
The remote host is missing one of the following rollup KBs :

Cumulative
  - 5039889

C:\Windows\Microsoft.NET\Framework\v4.0.30319\system.windows.forms.dll has not been patched.
    Remote version : 4.8.4654.0
    Should be      : 4.8.4739.0
```

180174 - WinRAR < 6.23 RCE

Synopsis

The remote Windows host has an application installed which is affected by a remote code execution vulnerability.

Description

The remote host is running WinRAR, an archive manager for Windows.

The version of WinRAR installed on the remote host is affected by a an improper validation of user-supplied data, which can result in memory access past the end of an allocated buffer which can be exploited remotely and may allow attackers to execute code in the context of the current process.

See Also

https://www.zerodayinitiative.com/advisories/ZDI-23-1152/

https://www.rarlab.com/rarnew.htm

Solution

Upgrade to WinRAR version 6.23 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2023-38831
CVE	CVE-2023-40477
XREF	CISA-KNOWN-EXPLOITED:2023/09/14
XREF	IAVA:2023-A-0436-S

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2023/08/24, Modified: 2024/05/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\WinRAR\WinRAR.exe
Installed version : 6.22.0.0
Fixed version     : 6.23
```

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

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

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: 2023/12/26

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.
```

103569 - Windows Defender Antimalware/Antivirus Signature Definition Check

Synopsis

Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old

Description

Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day.

See Also

https://www.microsoft.com/en-us/wdsi/definitions

Solution

Trigger an update manually and/or enable auto-updates.

Risk Factor

High

Plugin Information

Published: 2017/10/02, Modified: 2024/08/06

Plugin Output

tcp/445/cifs

```
Malware Signature Timestamp : Aug. 17, 2024 at 22:49:57 GMT
Malware Signature Version   : 1.417.181.0
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

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: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
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 : CN=dc
|-Issuer  : CN=dc
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

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: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/3389/msrdp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=dc
```

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/3389/msrdp

```
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/3389/msrdp

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

192940 - WinRAR < 7.00 Multiple Vulnerabilities

Synopsis

The remote Windows host has an application installed which is affected by multiple vulnerabilities.

Description

The remote host is running WinRAR, an archive manager for Windows, whose reported version is prior to 7.00. It is, therefore, affected by multiple vulnerabilties:

- The vulnerability exists due to an error within the archive extraction functionality. A remote attacker can use a specially crafted archive to bypass the Mark-Of-The-Web protection mechanism and potentially compromise the affected system. (CVE-2024-30370)

- RARLAB WinRAR before 7.00, on Windows, allows attackers to spoof the screen output via ANSI escape sequences, a different issue than CVE-2024-33899. (CVE-2024-36052)

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

See Also

https://www.zerodayinitiative.com/advisories/ZDI-24-357/

https://www.rarlab.com/rarnew.htm

http://www.nessus.org/u?64afd272

Solution

Upgrade to WinRAR version 7.00 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2024-30370
CVE	CVE-2024-36052
XREF	IAVA:2024-A-0194-S
XREF	IAVA:2024-A-0303

Plugin Information

Published: 2024/04/05, Modified: 2024/05/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\WinRAR\WinRAR.exe
Installed version : 6.22.0.0
Fixed version     : 7.0
```

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

VPR Score

4.2

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: 2024/05/03

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 -32 seconds.
```

91231 - 7-Zip Installed

Synopsis

A compression utility is installed on the remote Windows host.

Description

7-Zip, a compressed archive manager, is installed on the remote Windows host.

See Also

https://www.7-zip.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0734

Plugin Information

Published: 2016/05/19, Modified: 2024/08/14

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files\7-Zip
Version : 22.1.0.0
```

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: 2023/10/05

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\4.18.24070.5-0\
  Version                      : 4.18.24070.5
  Engine version               : 1.1.24070.3
  Antivirus signature version  : 1.417.181.0
  Antispyware signature version : 1.417.181.0
```

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: 2024/08/14

Plugin Output

tcp/0

```
Vendor       : innotek GmbH
Version      : VirtualBox
Release date : 20061201000000.000000+000
UUID         : F63E4432-0172-49EA-A2F5-D667F03A2A6A
Secure boot  : disabled
```

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: 2024/07/31

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_server_2022 -> Microsoft Windows Server 2022

Following application CPE's matched on the remote system :

  cpe:/a:7-zip:7-zip:22.1.0.0 -> 7-Zip -
  cpe:/a:haxx:curl:8.7.0.0 -> Haxx Curl
  cpe:/a:microsoft:.net_framework:4.8 -> Microsoft .NET Framework
  cpe:/a:microsoft:.net_framework:4.8.4718.0 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:127.0.2651.105 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.1.20348.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_explorer:11.0.20348.2520 -> Microsoft Internet Explorer
  cpe:/a:microsoft:remote_desktop_connection:10.0.20348.2520 -> Microsoft Remote Desktop Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.24070.5 -> Microsoft System Center
 Endpoint Protection
  cpe:/a:microsoft:windows_app_store:1.15.0.20348
  cpe:/a:microsoft:windows_app_store:10.0.19580.1000
```

```
cpe:/a:microsoft:windows_app_store:10.0.19581.1000
cpe:/a:microsoft:windows_app_store:10.0.19585.1001
cpe:/a:microsoft:windows_app_store:10.0.19595.1001
cpe:/a:microsoft:windows_app_store:10.0.19640.1000
cpe:/a:microsoft:windows_app_store:10.0.20348.1
cpe:/a:microsoft:windows_app_store:10.0.20348.859
cpe:/a:microsoft:windows_app_store:10.0.4.1000
cpe:/a:microsoft:windows_app_store:1000.19580.1000.0
cpe:/a:microsoft:windows_app_store:1000.20348.1.0
cpe:/a:microsoft:windows_app_store:120.27512.10351.0
cpe:/a:microsoft:windows_app_store:14.0.27810.0
cpe:/a:microsoft:windows_app_store:2.21909.17002.0
cpe:/a:microsoft:windows_app_store:2.42007.9001.0
cpe:/a:microsoft:windows_app_store:6.2.1.0
cpe:/a:microsoft:windows_app_store:86.0.622.38
cpe:/a:microsoft:windows_defender:4.18.24070.5 -> Microsoft Windows Defender
cpe:/a:notepad-plus-plus:notepad%2b%2b:8.5.3.0 -> notepad-plus-plus Notepad++
cpe:/a:python:python:3.11.4150.1013 -> Python
cpe:/a:rarlab:winrar:6.22.0.0 -> RARLAB WinRAR
x-cpe:/a:microsoft:sysinternals_sysmon:14.16.0.0
```

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: 2024/08/14

Plugin Output

tcp/0

```
Computer Manufacturer : innotek GmbH
Computer Model : VirtualBox
Computer Type : Other

Computer Physical CPU's : 1
Computer Logical CPU's  : 3
  CPU0
    Architecture  : x64
    Physical Cores: 3
    Logical Cores : 3

Computer Memory : 5119 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: 2024/08/14

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path          : c:\windows\system32\curl.exe
  Version       : 8.7.0.0
  Managed by OS : True

  Path          : c:\windows\syswow64\curl.exe
  Version       : 8.7.0.0
  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 : samss 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 : SidKey Local End Point

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 : protected_storage

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 : lsasspirpc

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 : lsapolicylookup

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 : LSA_EAS_ENDPOINT

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 : LSA_IDPEXT_ENDPOINT

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 : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc  [...]
```

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 : 338cd001-2244-31f1-aaaa-900038001003, version 1.0
Description : Remote Registry
Windows process : svchost.exe
Annotation : RemoteRegistry Interface
Type : Remote RPC service
Named pipe : \PIPE\winreg
Netbios name : \\DC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : da5a86c5-12c2-4943-ab30-7f74a813d853, version 1.0
Description : Unknown RPC service
Annotation : RemoteRegistry Perflib Interface
Type : Remote RPC service
Named pipe : \PIPE\winreg
Netbios name : \\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 : \\DC

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

```
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\SessEnvPublicRpc
Netbios name : \\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 : \\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 : \\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 : \\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 : \\DC

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

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 : 192.168.56.50

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 : 192.168.56.50

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 : 49664
IP : 192.168.56.50

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 : 49664
IP : 192.168.56.50
```

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 : 192.168.56.50
```

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 : 192.168.56.50
```

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 : 192.168.56.50

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 : 192.168.56.50
```

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 : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.56.50
```

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/49669/dce-rpc

```
The following DCERPC services are available on TCP port 49669 :

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 : 49669
IP : 192.168.56.50

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 : 49669
IP : 192.168.56.50

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 : 49669
IP : 192.168.56.50

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 : 49669
IP : 192.168.56.50

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 : 49669
IP : 192.168.56.50
```

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/49672/dce-rpc

```
The following DCERPC services are available on TCP port 49672 :

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 : 49672
IP : 192.168.56.50
```

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/49678/dce-rpc

```
The following DCERPC services are available on TCP port 49678 :

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 : 49678
IP : 192.168.56.50
```

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: 2024/08/14

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 : 5/8/2021 9:36 AM

Package      : Downlevel-NLS-Sorting-Versions-Server-FoD-
Package~31bf3856ad364e35~wow64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 5/8/2021 9:36 AM

Package      : Microsoft-OneCore-DirectX-Database-FOD-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 5/8/2021 9:36 AM

Package      : Microsoft-OneCore-RasSstp-Api-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Staged
Release Type : Feature Pack
Install Time :

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

```
State        : Installed
Release Type : Feature Pack
Install Time : 5/8/2021 9:35 AM

Package      : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : Foundation
Install Time : 5/8/2021 8:24 AM

Package      : Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~11.0.20348.2520
State        : Installed
Release Type : OnDemand Pack
Install Time : 6/27/2024 7:48 AM

Package      : Microsoft-Windows-LanguageFeatures-Basic-en-us-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 5/8/2021 9:35 AM

Package      : Microsoft-Windows-LanguageFeatures-Handwriting-en-us-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 5/8/2021 9:36 AM

Package      : Microsoft-Windows-LanguageFeatures-OCR-en-us-
Package~31bf3856ad364e35~amd64~~10.0.20348.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 5/8/2021 9:36 AM

Package      : Microsoft-Windows-LanguageFeatures-Speech-en-us-Package~31bf3856ad364e35~amd64~~10.0.
 [...]
```

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: 2024/08/14

Plugin Output

tcp/0

```
Hostname : DC
  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: 2022/09/09

Plugin Output

tcp/0

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

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/12/06, Modified: 2024/08/14

Plugin Output

tcp/0

```
Group Name : Access Control Assistance Operators
Host Name  : DC
Group SID  : S-1-5-32-579
Members    :

Group Name : Administrators
Host Name  : DC
Group SID  : S-1-5-32-544
Members    :
  Name : Administrator
    Domain : DC
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3043820608-1980768537-1953574876-500
  Name : vagrant
    Domain : DC
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3043820608-1980768537-1953574876-1000

Group Name : Backup Operators
Host Name  : DC
Group SID  : S-1-5-32-551
Members    :

Group Name : Certificate Service DCOM Access
Host Name  : DC
Group SID  : S-1-5-32-574
Members    :

Group Name : Cryptographic Operators
Host Name  : DC
Group SID  : S-1-5-32-569
Members    :
```

```
Group Name : Device Owners
Host Name  : DC
Group SID  : S-1-5-32-583
Members    :

Group Name : Distributed COM Users
Host Name  : DC
Group SID  : S-1-5-32-562
Members    :

Group Name : Event Log Readers
Host Name  : DC
Group SID  : S-1-5-32-573
Members    :

Group Name : Guests
Host Name  : DC
Group SID  : S-1-5-32-546
Members    :
  Name : Guest
    Domain : DC
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3043820608-1980768537-1953574876-501

Group Name : Hyper-V Administrators
Host Name  : DC
Group SID  : S-1-5-32-578
Members    :

Group Name : IIS_IUSRS
Host Name  : DC
Group SID  : S-1-5-32-568
Members    :
  Name : IUSR
    Domain : DC
    Class  : Win32_SystemAccount
    SID    : S-1-5-17

Group Name : Network Configuration Operators
Host Name  : DC
Group SID  : S-1-5-32-556
Members    :

Group Name : Performance Log Users
Host Name  : DC
Group SID  : S-1-5-32-559
Members    :

Group Name : Performance Monitor Users
Host Name  : DC
Group SID  : S-1-5-32-558
Members    :

Group Name : Power Users
Host Name  : DC
Group SID  : S-1-5-32-547
Members    :

Group Name : Print Operators
Host Name  : DC
Group SID  : S-1-5-32-550
Members    :

Group Name : RDS Endpoint Servers
Host Name  : DC
Group SID  : S-1-5-32-576
Members    :

Group Name : RDS Management Servers
```

```
Host Name  : DC
G [...]
```

72684 - Enumerate Users via WMI

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI.

Description

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI. Only identities that the authenticated SMB user has permissions to view will be retrieved by this plugin.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/02/25, Modified: 2024/08/14

Plugin Output

tcp/0

```
Name            : Administrator
SID             : S-1-5-21-3043820608-1980768537-1953574876-500
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : DefaultAccount
SID             : S-1-5-21-3043820608-1980768537-1953574876-503
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Guest
SID             : S-1-5-21-3043820608-1980768537-1953574876-501
Disabled        : True
Lockout         : False
Change password : False
Source          : Local

Name            : vagrant
SID             : S-1-5-21-3043820608-1980768537-1953574876-1000
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : WDAGUtilityAccount
```

```
SID             : S-1-5-21-3043820608-1980768537-1953574876-504
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

No. Of Users : 5
```

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: 2024/08/14

Plugin Output

tcp/0

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

C:\Python311\Scripts\
C:\Python311\
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\ProgramData\chocolatey\bin
C:\Users\vagrant\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:AA:5F:7A : PCS Systemtechnik GmbH
08:00:27:40:99:73 : 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: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:AA:5F:7A
  - 08:00:27:40:99:73
```

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/47001/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

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: Tue, 20 Aug 2024 20:51:20 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/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: Tue, 20 Aug 2024 20:51:20 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: 2024/08/14

Plugin Output

tcp/0

```
+ Ethernet 3
  + IPv4
    - Address       : 192.168.56.50
      Assign Method : static
+ Loopback Pseudo-Interface 1
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ Ethernet 4
  + IPv4
    - Address       : 10.0.2.15
      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: 2024/08/14

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

Internet Explorer typed URL report attached.
```

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 '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.
```

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\winhttp.dll,-100 : WinHTTP Web Proxy Auto-Discovery Service
@%systemroot%\system32\themeservice.dll,-8192 : Themes
@%systemroot%\system32\mprmsg.dll,-32011 : Remote Access IP ARP Driver
@%systemroot%\system32\tabsvc.dll,-100 : Touch Keyboard and Handwriting Panel Service
@%systemroot%\system32\windows.devices.picker.dll,-1006 : DevicePicker
@%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.
@%systemroot%\system32\icsvc.dll,-201 : Hyper-V Data Exchange Service
c:\windows\system32,@elscore.dll,-8 : Microsoft Malayalam to Latin Transliteration
@%systemroot%\system32\icsvcvss.dll,-101 : Hyper-V Volume Shadow Copy Requestor
@%systemroot%\system32\devicesflowbroker.dll,-103 : DevicesFlow
@%systemroot%\system32\msimsg.dll,-27 : Windows Installer
@%systemroot%\system32\rmapi.dll,-1001 : Radio Management Service
@%systemroot%\system32\drivers\winnat.sys,-10001 : Windows NAT Driver
@%systemroot%\system32\drivers\afd.sys,-1000 : Ancillary Function Driver for Winsock
@%systemroot%\system32\userdataaccessres.dll,-14000 : Provides apps access to structured user
 data, including contact info, calendars, messages, and other content. If you stop or disable this
 service, apps that use this data might not work correctly.
@%systemroot%\system32\das.dll,-100 : Device Association Service
@regsvc.dll,-1 : Remote Registry
```

```
@%systemroot%\system32\tieringengineservice.exe,-701 : Optimizes the placement of data in storage
 tiers on all tiered storage spaces in the system.
@%systemroot%\system32\drivers\tunnel.sys,-500 : Microsoft Tunnel Miniport Adapter Driver
@%systemroot%\system32\vssvc.exe,-102 : Volume Shadow Copy
@%systemroot%\system32\drivers\ehstorclass.sys,-100 : Enhanced Storage Filter Driver
@ [...]
```

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: 2022/10/18

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: 2024/07/12

Plugin Output

tcp/445/cifs

```
  Path                          : C:\Windows\Microsoft.NET\Framework
\v4.0.30319\system.runtime.serialization.dll
  Version                       : 4.8.4718.0
  .NET Version                  : 4.8
  Associated KB                 : 5036613
  Latest effective update level : 04_2024
```

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: 2024/08/14

Plugin Output

tcp/445/cifs

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

    Name    : unknown
    Version : 1.79.1
    Path    : C:\Users\vagrant\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.79.1_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\vagrant\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: 2024/08/14

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 127.0.2651.105
```

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: 2024/08/14

Plugin Output

tcp/445/cifs

```
Type       : Admin Groups
Is Enabled : False

Type       : User Groups
Is Enabled : False
```

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: 2024/08/14

Plugin Output

tcp/0

```
Path    : C:\Windows\system32\mshtml.dll
Version : 11.0.20348.2520
```

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
```

66424 - Microsoft Malicious Software Removal Tool Installed

Synopsis

An antimalware application is installed on the remote Windows host.

Description

The Microsoft Malicious Software Removal Tool is installed on the remote host. This tool is an application that attempts to detect and remove known malware from Windows systems.

See Also

http://www.nessus.org/u?47a3e94d

https://support.microsoft.com/en-us/help/891716

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/05/15, Modified: 2023/01/10

Plugin Output

tcp/445/cifs

```
File               : C:\Windows\system32\MRT.exe
Version            : 5.125.24060.1001
Release at last run : unknown
Report infection information to Microsoft : Yes
```

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 : 10.0.20348.2520
```

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: 2023/06/26

Plugin Output

tcp/445/cifs

```
Cumulative Rollup : 06_2024 [KB5039227]
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 : 06_2024
  File checked                  : C:\Windows\system32\ntoskrnl.exe
  File version                  : 10.0.20348.2520
  Associated KB                 : 5039227
```

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 :

  - DC\Administrator (User)
  - DC\vagrant (User)
```

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
```

10913 - Microsoft Windows - Local Users Information : Disabled Accounts

Synopsis

At least one local user account has been disabled.

Description

Using the supplied credentials, Nessus was able to list local user accounts that have been disabled.

Solution

Delete accounts that are no longer needed.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local user account has been disabled :

  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10914 - Microsoft Windows - Local Users Information : Never Changed Passwords

Synopsis

At least one local user has never changed his or her password.

Description

Using the supplied credentials, Nessus was able to list local users who have never changed their passwords.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2019/07/08

Plugin Output

tcp/0

```
The following local user has never changed his/her password :\n
  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10916 - Microsoft Windows - Local Users Information : Passwords Never Expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local users have passwords that never expire :

  - Administrator
  - vagrant


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

10915 - Microsoft Windows - Local Users Information : User Has Never Logged In

Synopsis

At least one local user has never logged into his or her account.

Description

Using the supplied credentials, Nessus was able to list local users who have never logged into their accounts.

Solution

Delete accounts that are not needed.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local users have never logged in :

  - Administrator
  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

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: 2024/08/14

Plugin Output

tcp/0

```
192.168.56.1 : 0a-00-27-00-00-10
192.168.56.34 : 08-00-27-62-96-0d
192.168.56.255 : 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
10.0.2.2 : 52-54-00-12-35-02
10.0.2.3 : 52-54-00-12-35-03
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

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: 2024/08/14

Plugin Output

tcp/0

```
    3.au.download.windowsupdate.com
    config.edge.skype.com
    cp601.prod.do.dsp.mp.microsoft.com
    ctldl.windowsupdate.com
    download.windowsupdate.com
    fe2cr.update.microsoft.com
    fe3cr.delivery.mp.microsoft.com
    fe3cr.delivery.mp.microsoft.com
    geo.prod.do.dsp.mp.microsoft.com
    go.microsoft.com
    kv601.prod.do.dsp.mp.microsoft.com
    login.live.com
    msedge.api.cdp.microsoft.com
    ocsp.digicert.com
    settings-win.data.microsoft.com
    slscr.update.microsoft.com
    slscr.update.microsoft.com
    storecatalogrevocation.storequality.microsoft.com
    time.windows.com
    tsfe.trafficshaping.dsp.mp.microsoft.com
    v10.events.data.microsoft.com
    wdcp.microsoft.com
    www.telecommandsvc.microsoft.com

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 : 25
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 3
  username : SYSTEM
  os : Windows_NT
  chocolateyinstall : C:\ProgramData\chocolatey
  temp : %SystemRoot%\TEMP
  processor_revision : 2102
  path : C:\Python311\Scripts\;C:\Python311\;%SystemRoot%\system32;%SystemRoot%;%SystemRoot%
\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\;C:
\ProgramData\chocolatey\bin;
  tmp : %SystemRoot%\TEMP
  processor_identifier : AMD64 Family 25 Model 33 Stepping 2, AuthenticAMD
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-3043820608-1980768537-1953574876-1000
    temp : %USERPROFILE%\AppData\Local\Temp
```

```
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
    tmp : %USERPROFILE%\AppData\Local\Temp
    chocolateylastpathupdate : 133311812820940607
```

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: 2024/07/31

Plugin Output

tcp/0

```
OS Name      : Microsoft Windows Server 2022 21H2
Vendor       : Microsoft
Product      : Windows Server
Release      : 2022 21H2
Edition      : Standard
Version      : 10.0.20348.2527
Role         : server
Kernel       : Windows NT 10.0
Architecture : x64
CPE v2.2     : cpe:/o:microsoft:windows_server_2022:10.0.20348.2527:-
CPE v2.3     : cpe:2.3:o:microsoft:windows_server_2022:10.0.20348.2527:-:*:*:standard:*: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 :

7-Zip 22.01 (x64)  [version 22.01]
BusinessObjects BI version 430  [version 430]  [installed on 2023/06/14]
Dell Wyse Management Suite version 3.6.1  [version 3.6.1]  [installed on 2023/06/14]
Magical Jelly Bean KeyFinder  [version 2.0.10.13]  [installed on 2023/06/14]
Metabase version 1.40.4  [version 1.40.4]  [installed on 2023/06/14]
Microsoft Edge  [version 127.0.2651.105]  [installed on 2024/08/18]
Microsoft Edge Update  [version 1.3.195.15]
Notepad++ (64-bit x64)  [version 8.5.3]
Oracle VM VirtualBox Guest Additions 7.0.8  [version 7.0.8.156879]
Photoshop version 23.3.2  [version 23.3.2]  [installed on 2023/06/14]
Process Hacker 2.39 (r124)  [version 2.39.0.124]  [installed on 2023/06/14]
Rocket League version 0.0.3  [version 0.0.3]  [installed on 2023/06/14]
WinRAR 6.22 (64-bit)  [version 6.22.0]
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532  [version 14.36.32532]  [installed on
 2023/06/14]
Python 3.11.4 Development Libraries (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
```

```
Python Launcher  [version 3.11.4150.0]  [installed on 2023/06/14]
Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532  [version 14.36.32532.0]
Python 3.11.4 Test Suite (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
Wazuh Agent  [version 4.3.10]  [installed on 2023/06/14]
Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532  [version 14.36.32532]  [installed on
 2023/06/14]
Python 3.11.4 Add to Path (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
Python 3.11.4 Standard Library (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532  [version 14.36.32532.0]
Python 3.11.4 Utility Scripts (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
Python 3.11.4 Tcl/Tk Support (64-bit)  [version 3.11.4150.0]  [installed on 2023/06/14]
Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532  [version 14.36.32532]  [installed on
 2023/06/14]
 [...]
```

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 :

 - Python 3.11.4 pip Bootstrap (64-bit)
     Best Confidence Version  : 3.11.4150.0
     Version Confidence Level : 2
     All Possible Versions    :  81.5.26260, 3.11.4150.0
     Other Version Data
       [VersionMajor] :
           Raw Value           : 3
       [Version] :
           Raw Value           : 51056694
           Parsed Version : 81.5.26260
       [DisplayName] :
           Raw Value           : Python 3.11.4 pip Bootstrap (64-bit)
       [UninstallString] :
           Raw Value           : MsiExec.exe /I{D86BDA9F-D389-445E-B3E6-C35EF9FD41C7}
       [InstallDate] :
           Raw Value           : 2023/06/14
       [DisplayVersion] :
           Raw Value           : 3.11.4150.0
       [Publisher] :
           Raw Value           : Python Software Foundation
```

```
      [VersionMinor] :
          Raw Value           : 11

- BusinessObjects BI version 430
    Best Confidence Version  : 51.1052.0.0
    Version Confidence Level : 3
    All Possible Versions    :  51.1052.0.0, 430
    Other Version Data
      [VersionMajor] :
          Raw Value           : 430
      [InstallLocation] :
          Raw Value           : C:\Program Files (x86)\SAP\
      [DisplayName] :
          Raw Value           : BusinessObjects BI version 430
      [UninstallString] :
          Raw Value           : "C:\Program Files (x86)\SAP\unins000.exe"
          Parsed File Path    : C:\Program Files (x86)\SAP\unins000.exe
          Parsed File Version : 51.1052.0.0
      [InstallDate] :
          Raw Value           : 2023/06/14
      [DisplayVersion] :
          Raw Value           : 430
      [VersionMinor] :
          Raw Value           : 0

- Wazuh Agent
    Best Confidence Version  : 4.3.10
    Version Confidence Level : 2
    All Possible Versions    :  103.48.21634, 4.3.10
    Other Version Data
      [VersionMajor] :
          Raw Value           : 4
      [Version] :
          Raw Value           : 67305482 [...]
```

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 : 2024-08-18T16:38:00+10:00 (20240818163800.449302+600)
```

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 enuemrate the SIDs of logged on users

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/05/25, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Logged on users :
  - S-1-5-21-3043820608-1980768537-1953574876-1000
    Domain   : DC
    Username : vagrant
```

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     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#2&1f4adffe&0&000001#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004d0073006600740026005000720 06f006400 5

  Name     : \??\volume{393f2858-0a98-11ee-9c23-080027409973}
  Data     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#2&1f4adffe&0&000001#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004d0073006600740026005000720 06f006400 5

  Name     : \dosdevices\d:
  Data     : \??\IDE#CdRomVBOX_CD-
ROM_____1.0_____#5&394c0ad3&0&0.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0049004400450023004300640052006f006d00560042004f0058005f00430044002d0052004f004d005f005f005f005f005

  Name     : \??\volume{e399adf2-6cea-11ed-9c1c-806e6f6e6963}
  Data     : \??\FDC#GENERIC_FLOPPY_DRIVE#5&34923401&0&0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data : 5c003f003f005c0046004400430023004700450 04e00450 [...]
```

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: 2024/08/14

Plugin Output

tcp/0

```
NBT information attached.
First 10 lines of all CSVs:
nbtstat_local.csv:
Interface,Name,Suffix,Type,Status,MAC
192.168.56.50,DC,<00>,UNIQUE,Conflict,08:00:27:AA:5F:7A
192.168.56.50,DC,<20>,UNIQUE,Conflict,08:00:27:AA:5F:7A
192.168.56.50,WORKGROUP,<00>,GROUP,Registered,08:00:27:AA:5F:7A
```

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 Network Connection
Network Adapter Driver Version     : 8.4.13.0

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

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: 2024/08/14

Plugin Output

tcp/0

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (368)
 0 : Registry (112)
 1 : explorer.exe (4488)
 1 : |- VBoxTray.exe (5764)
 1 : |- AzureArcSysTray.exe (5900)
 0 : csrss.exe (476)
 1 : csrss.exe (548)
 0 : wininit.exe (572)
 0 : |- services.exe (688)
 0 :    |- svchost.exe (1004)
 0 :    |- svchost.exe (1068)
 0 :    |- svchost.exe (1144)
 0 :    |- svchost.exe (1160)
 0 :    |- svchost.exe (1308)
 0 :    |- svchost.exe (1336)
 0 :    |- svchost.exe (1364)
 0 :    |- svchost.exe (1444)
 0 :    |- svchost.exe (1468)
 0 :       |- taskhostw.exe (2916)
 1 :       |- taskhostw.exe (4344)
 0 :       |- MicrosoftEdgeUpdate.exe (4588)
 0 :    |- svchost.exe (1540)
 0 :    |- svchost.exe (1560)
 1 :       |- sihost.exe (4432)
```

```
0 :    |- svchost.exe (1584)
0 :    |- svchost.exe (1612)
0 :    |- svchost.exe (1696)
0 :    |- svchost.exe (1752)
0 :    |- svchost.exe (1760)
0 :    |- VBoxService.exe (1772)
0 :    |- svchost.exe (1816)
0 :    |- svchost.exe (1828)
0 :    |- svchost.exe (1836)
0 :    |- svchost.exe (2004)
0 :    |- svchost.exe (2016)
0 :    |- svchost.exe (2064)
0 :    |- svchost.exe (2096)
0 :    |- svchost.exe (2104)
0 :    |- svchost.exe (2140)
0 :    |- svchost.exe (2164)
0 :    |- svchost.exe (2188)
0 :    |- svchost.exe (2296)
0 :    |- svchost.exe (2400)
0 :    |- svchost.exe (2408)
0 :    |- svchost.exe (2468)
0 :    |- TrustedInstaller.exe (2496)
0 :    |- spoolsv.exe (2536)
0 :    |- svchost.exe (2552)
0 :    |- svchost.exe (2564)
0 :    |- svchost.exe (2636)
0 :    |- svchost.exe (2672)
0 :    |- svchost.exe (2724)
0 :       |- AggregatorHost.exe (3780)
0 :    |- svchost.exe (2732)
0 :    |- svchost.exe (2740)
0 :    |- svchost.exe (2752)
0 :    |- svchost.exe (2776)
0 :    |- svchost.exe (2788)
0 :    |- Sysmon64.exe (2820)
0 :    |- svchost.exe (2852)
0 :    |- svchost.exe (2860)
0 :    |- svchost.exe (2868)
0 :    |- svchost.exe (2876)
[...]
```

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: 2024/08/14

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: 2024/08/14

Plugin Output

udp/123

```
The Win32 process 'svchost.exe' is listening on this port (pid 2876).

This process 'svchost.exe' (pid 2876) 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: 2024/08/14

Plugin Output

tcp/135/epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 956).

This process 'svchost.exe' (pid 956) 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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

Plugin Output

udp/500

```
The Win32 process 'svchost.exe' is listening on this port (pid 2400).

This process 'svchost.exe' (pid 2400) 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: 2024/08/14

Plugin Output

tcp/3389/msrdp

```
The Win32 process 'svchost.exe' is listening on this port (pid 452).

This process 'svchost.exe' (pid 452) is hosting the following Windows services :
TermService (@%SystemRoot%\System32\termsrv.dll,-268)
```

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: 2024/08/14

Plugin Output

udp/3389

```
The Win32 process 'svchost.exe' is listening on this port (pid 452).

This process 'svchost.exe' (pid 452) is hosting the following Windows services :
TermService (@%SystemRoot%\System32\termsrv.dll,-268)
```

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: 2024/08/14

Plugin Output

udp/3702

```
The Win32 process 'svchost.exe' is listening on this port (pid 3352).

This process 'svchost.exe' (pid 3352) 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: 2024/08/14

Plugin Output

udp/4500

```
The Win32 process 'svchost.exe' is listening on this port (pid 2400).

This process 'svchost.exe' (pid 2400) 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: 2024/08/14

Plugin Output

udp/5353

```
The Win32 process 'svchost.exe' is listening on this port (pid 2096).

This process 'svchost.exe' (pid 2096) 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: 2024/08/14

Plugin Output

udp/5355/llmnr

```
The Win32 process 'svchost.exe' is listening on this port (pid 2096).

This process 'svchost.exe' (pid 2096) 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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

Plugin Output

tcp/49664/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 696).

This process 'lsass.exe' (pid 696) is hosting the following Windows services :
KeyIso (@keyiso.dll,-100)
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: 2024/08/14

Plugin Output

tcp/49665/dce-rpc

```
The Win32 process 'wininit.exe' is listening on this port (pid 572).
```

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: 2024/08/14

Plugin Output

tcp/49666/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1144).

This process 'svchost.exe' (pid 1144) 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: 2024/08/14

Plugin Output

tcp/49667/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1468).

This process 'svchost.exe' (pid 1468) 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: 2024/08/14

Plugin Output

tcp/49668/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 2064).

This process 'svchost.exe' (pid 2064) is hosting the following Windows services :
SessionEnv (@%SystemRoot%\System32\SessEnv.dll,-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: 2024/08/14

Plugin Output

tcp/49669/dce-rpc

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 2536).

This process 'spoolsv.exe' (pid 2536) 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: 2024/08/14

Plugin Output

tcp/49672/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 2408).

This process 'svchost.exe' (pid 2408) 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: 2024/08/14

Plugin Output

tcp/49678/dce-rpc

```
The Win32 process 'services.exe' is listening on this port (pid 688).
```

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: 2024/08/14

Plugin Output

tcp/50131

```
The Win32 process 'svchost.exe' is listening on this port (pid 2868).

This process 'svchost.exe' (pid 2868) 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: 2024/08/14

Plugin Output

udp/60507

```
The Win32 process 'svchost.exe' is listening on this port (pid 2096).

This process 'svchost.exe' (pid 2096) 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: 2024/08/14

Plugin Output

udp/61454

```
The Win32 process 'svchost.exe' is listening on this port (pid 3352).

This process 'svchost.exe' (pid 3352) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
```

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: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
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 : .\vagrant
```

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: 2024/07/29

Plugin Output

tcp/445/cifs

```
- The SMB tests will be done as vagrant/******
```

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-1-5-21-3043820608-1980768537-1953574876

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

```
Nessus was able to obtain the following information about the host, by
parsing the SMB2 Protocol's NTLM SSP message:

Target Name: DC
NetBIOS Domain Name: DC
NetBIOS Computer Name: DC
DNS Domain Name: dc
DNS Computer Name: dc
DNS Tree Name: unknown
Product Version: 10.0.20348
```

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
```

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 :

  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_6718e startup parameters :
  Display name : CDPUserSvc_6718e
  Service name : CDPUserSvc_6718e
  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/

DPS startup parameters :
  Display name : Diagnostic Policy Service
  Service name : DPS
  Log on as : NT AUTHORITY\LocalService
  Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p

DcomLaunch startup parameters :
  Display name : DCOM Server Process Launcher
  Service name : DcomLaunch
  Log on as : LocalSystem
  Executable path : C:\Windows\system32\svchost.exe -k DcomLaunch -p

Dhcp startup parameters :
  Display  [...]
```

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 :

Base Filtering Engine [ BFE ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Capability Access Manager Service [ camsvc ]
Connected Devices Platform Service [ CDPSvc ]
Certificate Propagation [ CertPropSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Data Sharing Service [ DsSvc ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Function Discovery Provider Host [ fdPHost ]
Function Discovery Resource Publication [ FDResPub ]
```

```
Windows Font Cache Service [ FontCache ]
Group Policy Client [ gpsvc ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
IP Helper [ iphlpsvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Windows License Manager Service [ LicenseManager ]
TCP/IP NetBIOS Helper [ lmhosts ]
Local Session Manager [ LSM ]
Windows Defender Firewall [ mpssvc ]
Distributed Transaction Coordinator [ MSDTC ]
Network Connection Broker [ NcbService ]
Network List Service [ netprofm ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Program Compatibility Assistant Service [ PcaSvc ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
Remote Access Connection Manager [ RasMan ]
Remote Registry [ RemoteRegistry ]
RPC Endpoint Mapper [ RpcEptMapper ]
Remote Procedure Call (RPC) [ RpcSs ]
Security Accounts Manager [ SamSs ]
Task Scheduler [ Schedule ]
System Event Notification Service [ SENS ]
Remote Desktop Configuration [ SessionEnv ]
Shell Hardware Detection [ ShellHWDetection ]
Print Spooler [ Spooler ]
Secure Socket Tunneling Protocol Service [ SstpSvc ]
State Repository Service [ StateRepository ]
Storage Service [ StorSvc ]
SysMain [  [...]
```

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: 2024/08/14

Plugin Output

tcp/0

```
vagrant

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
    - C:\Tools\AtomicRedTeam\atomics\T1218\src\T1218Test.docx
    - C:\Tools\AtomicRedTeam\atomics\T1221\src\Calculator.docx
    - C:\Tools\AtomicRedTeam\atomics\T1559.002\bin\DDE_Document.docx
```

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 : \\DC\pslogs
Local path : c:\pslogs
[*] Allow ACE for Everyone (S-1-1-0): 0x001301bf
    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 vagrant :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
ADFS
appcompat
apppatch
AppReadiness
assembly
AzureArcSetup
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
BrowserCore
CbsTemp
Containers
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
drivers
```

```
DtcInstall.log
ELAMBKUP
en-US
explorer.exe
Fonts
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IME
ImmersiveControlPanel
INF
InputMethod
Installer
L2Schemas
LiveKernelReports
Logs
lsasetup.log
Media
mib.bin
Microsoft.NET
Migration
ModemLogs
notepad.exe
OCR
Offline Web Pages
Panther
Performance
PFRO.log
PLA
PolicyDefinitions
Prefetch
PrintDialog
Provisioning
py.exe
pyshellext.amd64.dll
pyw.exe
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServerStandard.xml
ServiceProfiles
ServiceState
servicing
Setup
ShellComponents
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
Sysmon64.exe
SysmonDrv.sys
System
system.ini
System32
SystemApps
SystemResources
SystemTemp
SysWOW64
TAPI
Tasks
Temp
```

```
tracing
twain_32

- C$  - (readable,writable)
  + Content of this share :
$WinREAgent
bootTel.dat
Documents and Settings
DumpStack.log.tmp
found.000
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
pslogs
Python311
Recovery
Sysmon
System Volume Information
tmp
Tools
Users
vagrant
Windows

- pslogs  - (readable,writable)
  + Content of this share :
..
```

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 vagrant:

  - ADMIN$
  - C$
  - IPC$
  - pslogs
```

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 :
  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: 2024/08/14

Plugin Output

tcp/445/cifs

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

 - Autoruns.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Autoruns.lnk
     Target       : C:\Tools\Sysinternals\Autoruns64.exe
     Version      : 14.0.9.0

 - 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

 - Immersive Control Panel.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Immersive Control
 Panel.lnk
     Target       : C:\Windows\System32\Control.exe
     Version      : 10.0.20348.350

 - 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      : 127.0.2651.105
```

```
- Notepad++.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Notepad++.lnk
    Target       : C:\Program Files\Notepad++\notepad++.exe
    Version      : 8.5.3.0

- Process Explorer.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Process Explorer.lnk
    Target       : C:\Tools\Sysinternals\procexp64.exe
    Version      : 17.4.0.0

- Process Monitor.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Process Monitor.lnk
    Target       : C:\Tools\Sysinternals\Procmon.exe
    Version      : 3.94.0.0

- 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

- Tcpview.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Tcpview.lnk
    Target       : C:\Tools\Sysinternals\Tcpview.exe
    Version      : 4.19.0.0

- 7-Zip File Manager.lnk
    .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\7-Zip\7-Zip File Manager.
[...]
```

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
  VBoxTray - %SystemRoot%\system32\VBoxTray.exe
  bginfo - wscript
```

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 :

  - KB5039889 ( https://support.microsoft.com/en-us/help/5039889 )
  - KB5040437 ( https://support.microsoft.com/en-us/help/5040437 )
  - KB5041160 ( https://support.microsoft.com/en-us/help/5041160 )
```

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 : E. Australia Standard
 Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-682
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-681
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 : 0xFFFFFDA8
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0xFFFFFDA8
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000000000000000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000000000000000000000000000000
```

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: 2024/08/05

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.7
Nessus build : 20008
Plugin feed version : 202408201709
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Win2022_DavidStephens
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.56.34
Port scanner(s) : wmi_netstat
Port range : default
Ping RTT : 127.968 ms
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 '192.168.56.50\vagrant' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/8/21 6:49 AEST
Scan duration : 819 sec
Scan for malware : no
```

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: 2024/08/14

Plugin Output

tcp/0

```
Nessus was able to find 28 open ports.
```

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: 2024/08/14

Plugin Output

udp/123

```
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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

Plugin Output

tcp/3389/msrdp

```
Port 3389/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: 2024/08/14

Plugin Output

udp/3389

```
Port 3389/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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

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: 2024/08/14

Plugin Output

tcp/49669/dce-rpc

```
Port 49669/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: 2024/08/14

Plugin Output

tcp/49672/dce-rpc

```
Port 49672/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: 2024/08/14

Plugin Output

tcp/49678/dce-rpc

```
Port 49678/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: 2024/08/14

Plugin Output

tcp/50131

```
Port 50131/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: 2024/08/14

Plugin Output

udp/60507

```
Port 60507/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: 2024/08/14

Plugin Output

udp/61454

```
Port 61454/udp 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: 2024/08/14

Plugin Output

tcp/0

```
+ Network Interface Information :

 - Network Interface = [00000003] Intel(R) PRO/1000 MT Network Connection
 - MAC Address = 08:00:27:AA:5F:7A
 - IPAddress/IPSubnet = 192.168.56.50/255.255.255.0

+ Network Interface Information :

 - Network Interface = [00000004] Intel(R) PRO/1000 MT Network Connection
 - MAC Address = 08:00:27:40:99:73
 - IPAddress/IPSubnet = 10.0.2.15/255.255.255.0


+ 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
    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
    192.168.56.0    255.255.255.0   0.0.0.0
    192.168.56.50   255.255.255.255 0.0.0.0
    192.168.56.255  255.255.255.255 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
```

181646 - Notepad++ Installed (Windows)

Synopsis

Notepad++ is installed on the remote Windows host.

Description

Notepad++ is installed on the remote Windows host.

See Also

https://notepad-plus-plus.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/20, Modified: 2024/08/14

Plugin Output

tcp/0

```
Path    : C:\Program Files\Notepad++
Version : 8.5.3.0
```

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: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2022 Standard Build 20348
Confidence level : 100
Method : SMB_OS


The remote host is running Microsoft Windows Server 2022 Standard 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  : 192.168.56.50\vagrant
Protocol : SMB
```

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: 2024/07/15

Plugin Output

tcp/0

```
. You need to take the following 7 actions :

+ Install the following Microsoft patches :
- KB5041160
- KB5040437 (2 vulnerabilities)
- KB5039889

[ 7-Zip < 23.00 Multiple Vulnerabilities (180360) ]

+ Action to take : Upgrade to 7-Zip version 23.00 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Notepad++ < 8.5.7 Multiple Buffer Overflow Vulnerabilities (181867) ]

+ Action to take : Upgrade to Notepad++ 8.5.7 or later.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Security Updates for Microsoft .NET Framework (July 2024) (202304) ]
```

```
+ Action to take : Microsoft has released security updates for Microsoft .NET Framework.

[ WinRAR < 7.00 Multiple Vulnerabilities (192940) ]

+ Action to take : Upgrade to WinRAR version 7.00 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

139241 - Python Software Foundation Python Installed (Windows)

Synopsis

A programming language application is installed on the remote Windows host.

Description

Python, a tool to locally create and run application in the python programming language, is installed on the remote Windows host.

See Also

https://www.python.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/07/31, Modified: 2024/08/14

Plugin Output

tcp/0

```
Path    : C:\Python311\
Version : 3.11.4
```

122422 - RARLAB WinRAR Installed (Windows)

Synopsis

An archive manager is installed on the remote Windows host.

Description

RARLAB WinRaR, an archive manager, is installed on the remote Windows host.

See Also

https://www.rarlab.com/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0706

Plugin Information

Published: 2019/02/26, Modified: 2024/08/14

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files\WinRAR\WinRAR.exe
Version : 6.22.0.0
```

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\vagrant\AppData\Roaming\Microsoft\Windows\Recent\The Internet.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-1-5-21-3043820608-1980768537-1953574876-1000
C:\\$Recycle.Bin\\S-1-5-21-3043820608-1980768537-1953574876-1000\.
C:\\$Recycle.Bin\\S-1-5-21-3043820608-1980768537-1953574876-1000\..
C:\\$Recycle.Bin\\S-1-5-21-3043820608-1980768537-1953574876-1000\desktop.ini
```

10940 - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/09/11, Modified: 2022/02/01

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB5004330, Installed on: 2021/08/07
KB5037930, Installed on: 2024/06/27
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2023/02/28

Plugin Output

tcp/445/cifs

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - vagrant (id 1000)

Note that, in addition to the Administrator, Guest, and Kerberos
accounts, Nessus has enumerated local users with IDs between
1000 and 1200. To use a different range, edit the scan policy
and change the 'Enumerate Local Users: Start UID' and/or 'End UID'
preferences under 'Assessment->Windows' and re-run the scan. Only
UIDs between 1 and 2147483647 are allowed for this range.
```

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: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
This port supports TLSv1.0/TLSv1.1/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/3389/msrdp

```
Subject Name:

Common Name: dc

Issuer Name:

Common Name: dc

Serial Number: 27 1F 4B 10 9E 30 59 84 4F 02 59 97 C9 BF 94 77

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 16 07:33:31 2024 GMT
Not Valid After: Jan 15 07:33:31 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E3 23 8E E5 2F 47 E9 05 DB 2A B2 64 FF 6B 8F 6B 30 EF 65
            BE A7 84 61 1A FE 61 BD E7 81 A7 B5 B4 4B 6F 0E 41 A1 70 41
            CC 6A B0 3C 96 FD 2F 2B 0E 01 7E 03 6D 64 76 CD 45 8D 1D 6B
            C7 40 93 F6 43 50 34 5D 42 AE 88 75 4E C5 05 1F 67 A5 47 4F
            39 80 8D 79 00 CD AE E4 42 E6 0D BA 7F AE 5D D2 2A E3 F0 75
            53 8E DB 93 81 1F F4 34 77 DB 12 81 3E C9 C1 8F F3 49 A4 E3
            AD 60 11 04 01 1C FE 9D 9F D3 3E 5D 7B 75 70 4A C8 CD C0 2A
            17 A5 4A 2E AE 18 82 EC AC 81 36 EE E7 B4 20 BD 60 3F 63 9F
            DD 6F 06 B2 BD 54 FF 53 B1 C6 6A 41 D7 64 D7 C8 76 72 76 14
            39 5C 4B 06 26 2D 34 7D B7 BC 33 E9 B0 4E FE AC 76 5E A5 21
            DD C9 B2 89 0B 16 2D 95 12 BF 44 A4 69 60 A9 BE 0F 95 A9 C7
```

```
             1C 33 6B 66 62 20 7B 66 48 97 CB 76 13 CF 8E 5A 85 04 06 B2
             22 0F 5C 93 E2 15 9A 48 4A 4D 6E 4F 19 B4 E1 D3 49
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 76 1C F8 57 41 D1 FB 20 E5 7F 20 00 9D 69 4E 2E 8E F8 0D
           2C 5F 46 09 F3 C0 27 60 69 E0 C1 1C 44 4D 71 AC 92 9F C8 AB
           08 E0 3F B0 05 5C 25 5C CB B1 4E 18 CB 99 23 89 C6 68 E7 8A
           76 24 5E ED 5C 3E 6E 0E 61 9D C0 55 EA 63 8D 43 D2 1A F5 4F
           DA 76 BB 18 D5 A1 70 66 D0 06 DD 45 EB 4A 18 DF 8B BB FF 18
           26 E7 3D 14 95 FB 71 49 1E E7 78 CC 3F 93 C6 C3 F8 C5 42 70
           68 AC A7 9B 8E 8A DB 56 DA 5E 52 89 E5 0A D6 C3 64 F8 13 05
           F9 4D 80 CD 21 32 08 10 26 BF 00 97 F8 2D F4 19 7A F6 06 0D
           B7 6E BD 0E 8F 4F AC 7E 2A 8F FA A8 01 41 07 FB 1D 4B 29 96
           62 0E DF DB 39 AB 3E 65 F0 2A 94 EE 45 F0 5F [...]
```

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/3389/msrdp

```
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        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          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       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384     0xC0, 0x28       ECDH          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: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

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        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          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      ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH          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      ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C      RSA           RS [...]
```

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/3389/msrdp

```
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        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA       AES-CBC(128)
 SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          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}
```

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/3389/msrdp

```
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        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            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        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          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        ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          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} [...]
```

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: 2024/03/26

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: 2024/03/26

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: 2024/03/26

Plugin Output

tcp/47001/www

```
A web server is running on this port.
```

168261 - Sysmon Installed (Windows)

Synopsis

Sysmon is installed on the remote Windows host.

Description

Sysmon is installed on the remote Windows host.

Note: Thorough tests is required for this plugin to run.

See Also

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/29, Modified: 2024/08/14

Plugin Output

tcp/445/cifs

```
Path    : C:\Windows\Sysmon64.exe
Version : 14.16.0.0
```

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

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/3389/msrdp

```
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/3389/msrdp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/445/cifs

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       '192.168.56.50\vagrant'
Port:       445
Proto:      SMB
Method:     password
```

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:       '192.168.56.50\vagrant'
Port:       445
Proto:      SMB
Method:     password
```

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: dc

Issuer Name:

Common Name: dc

Serial Number: 27 1F 4B 10 9E 30 59 84 4F 02 59 97 C9 BF 94 77

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 16 07:33:31 2024 GMT
Not Valid After: Jan 15 07:33:31 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E3 23 8E E5 2F 47 E9 05 DB 2A B2 64 FF 6B 8F 6B 30 EF 65
            BE A7 84 61 1A FE 61 BD E7 81 A7 B5 B4 4B 6F 0E 41 A1 70 41
            CC 6A B0 3C 96 FD 2F 2B 0E 01 7E 03 6D 64 76 CD 45 8D 1D 6B
            C7 40 93 F6 43 50 34 5D 42 AE 88 75 4E C5 05 1F 67 A5 47 4F
            39 80 8D 79 00 CD AE E4 42 E6 0D BA 7F AE 5D D2 2A E3 F0 75
            53 8E DB 93 81 1F F4 34 77 DB 12 81 3E C9 C1 8F F3 49 A4 E3
            AD 60 11 04 01 1C FE 9D 9F D3 3E 5D 7B 75 70 4A C8 CD C0 2A
            17 A5 4A 2E AE 18 82 EC AC 81 36 EE E7 B4 20 BD 60 3F 63 9F
            DD 6F 06 B2 BD 54 FF 53 B1 C6 6A 41 D7 64 D7 C8 76 72 76 14
            39 5C 4B 06 26 2D 34 7D B7 BC 33 E9 B0 4E FE AC 76 5E A5 21
            DD C9 B2 89 0B 16 2D 95 12 BF 44 A4 69 60 A9 BE 0F 95 A9 C7
```

```
             1C 33 6B 66 62 20 7B 66 48 97 CB 76 13 CF 8E 5A 85 04 06 B2
             22 0F 5C 93 E2 15 9A 48 4A 4D 6E 4F 19 B4 E1 D3 49
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 76 1C F8 57 41 D1 FB 20 E5 7F 20 00 9D 69 4E 2E 8E F8 0D
           2C 5F 46 09 F3 C0 27 60 69 E0 C1 1C 44 4D 71 AC 92 9F C8 AB
           08 E0 3F B0 05 5C 25 5C CB B1 4E 18 CB 99 23 89 C6 68 E7 8A
           76 24 5E ED 5C 3E 6E 0E 61 9D C0 55 EA 63 8D 43 D2 1A F5 4F
           DA 76 BB 18 D5 A1 70 66 D0 06 DD 45 EB 4A 18 DF 8B BB FF 18
           26 E7 3D 14 95 FB 71 49 1E E7 78 CC 3F 93 C6 C3 F8 C5 42 70
           68 AC A7 9B 8E 8A DB 56 DA 5E 52 89 E5 0A D6 C3 64 F8 13 05
           F9 4D 80 CD 21 32 08 10 26 BF 00 97 F8 2D F4 19 7A F6 06 0D
           B7 6E BD 0E 8F 4F AC 7E 2A 8F FA A8 01 41 07 FB 1D 4B 29 96
           62 0E DF DB 39 AB 3E 65 F0 2A 94 EE 45 F0 5F [...]
```

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

```
20240818163800.449302+600
```

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 192.168.56.34 to 192.168.56.50 :
192.168.56.34
192.168.56.50

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\Public\Downloads\desktop.ini
C:\\Users\vagrant\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

```
vagrant
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\vagrant\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\vagrant\Downloads
  - recent : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\vagrant\Videos
  - my music : C:\Users\vagrant\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\vagrant\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\vagrant\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\vagrant\AppData\LocalLow
  - sendto : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\vagrant\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\vagrant\Documents
  - administrative tools : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
\Administrative Tools
  - startup : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\vagrant\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\vagrant\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\vagrant\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function instead
  - local appdata : C:\Users\vagrant\AppData\Local
  - my pictures : C:\Users\vagrant\Pictures
  - templates : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\vagrant\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\vagrant\Desktop
  - programs : C:\Users\vagrant\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  - fonts : C:\Windows\Fonts
  - cd burning : C:\Users\vag [...]
```

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

```
microsoft.windows.controlpanel
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\windows powershell\windows powershell.lnk
d:\vboxwindowsadditions-amd64.exe
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\file explorer.lnk
microsoft.windows.search_cw5n1h2txyewy!cortanaui
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\windowspowershell\v1.0\powershell.exe
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!app
simontatham.putty
d:\vboxwindowsadditions.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\paint.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\shutdown.exe
ueme_ctlcuacount:ctor
c:\users\vagrant\desktop\process hacker 2.lnk
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\microsoft edge.lnk
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\windows powershell.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\cmd.exe
msedge
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\snippingtool.exe
c:\tools\atomicredteam\atomics\t1555.003\bin\webbrowserpassview.exe
microsoft.windows.explorer
microsoft.autogenerated.{923dd477-5846-686b-a659-0fccd73851a8}
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\mspaint.exe
ueme_ctlsession
```

```
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\snipping tool.lnk
c:\users\vagrant\desktop\windows powershell.lnk
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
wj32.processhacker2
microsoft.autogenerated.{7511cb09-f4f0-9218-bb5e-de4d7c0fa759}

Extended userassist report attached.
```

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: 2024/08/14

Plugin Output

tcp/445/cifs

```
The remote host returned the following caption from Win32_OperatingSystem:

Microsoft Windows Server 2022 Standard
```

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: 2024/08/14

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB5037930
  - Description : Update
  - InstalledOn : 6/26/2024

+ KB5039227
  - Description : Security Update
  - InstalledOn : 6/27/2024

+ KB5039343
  - Description : Security Update
  - InstalledOn : 6/26/2024

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: 2024/08/14

Plugin Output

tcp/0

```
Nessus enumerated the following Windows features :

  - .NET Framework 4.8
  - .NET Framework 4.8 Features
  - Azure Arc Setup
  - File Server
  - File and Storage Services
  - File and iSCSI Services
  - Microsoft Defender Antivirus
  - Storage Services
  - System Data Archiver
  - TCP Port Sharing
```

```
    - WCF Services
    - Windows PowerShell
    - Windows PowerShell 5.1
    - WoW64 Support
```

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-1-5-21-3043820608-1980768537-1953574876-1000
```

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: 2024/08/14

Plugin Output

tcp/0

```
+ Computer System Product
  - IdentifyingNumber : 0
  - Description       : Computer System Product
  - Vendor            : innotek GmbH
  - Name              : VirtualBox
  - UUID              : F63E4432-0172-49EA-A2F5-D667F03A2A6A
  - 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: {f31247cf-018c-4f6a-a456-ffd46a721bd8}
Network Connection : Ethernet 4
DhcpNameServer: 10.0.2.3

Interface: Default
DhcpNameServer: 10.0.2.3
```

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: 2024/08/14

Plugin Output

tcp/0

```
Path                          : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24070.5-0\
Version                       : 4.18.24070.5
Engine Version                : 1.1.24070.3
Malware Signature Timestamp : Aug. 17, 2024 at 22:49:57 GMT
Malware Signature Version   : 1.417.181.0
Security Agent Identifier   : F9DAC7EE-920E-8E51-1430-A7771FBE93C0
Signatures Last Updated     : Aug. 18, 2024 at 06:45:12 GMT
```

164690 - Windows Disabled Command Prompt Enumeration

Synopsis

This plugin determines if the DisableCMD policy is enabled or disabled on the remote host for each local user.

Description

The remote host may employ the DisableCMD policy on a per user basis. Enumerated local users may have the following registry key:

'HKLM\Software\Policies\Microsoft\Windows\System\DisableCMD'

- Unset or 0: The command prompt is enabled normally.

- 1: The command promt is disabled.

- 2: The command prompt is disabled however windows batch processing is allowed.

See Also

http://www.nessus.org/u?b40698bc

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/09/06, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

```
Username: DefaultAccount
  SID: S-1-5-21-3043820608-1980768537-1953574876-503
  DisableCMD: Unset

Username: vagrant
  SID: S-1-5-21-3043820608-1980768537-1953574876-1000
  DisableCMD: Unset

Username: Administrator
  SID: S-1-5-21-3043820608-1980768537-1953574876-500
  DisableCMD: Unset

Username: WDAGUtilityAccount
  SID: S-1-5-21-3043820608-1980768537-1953574876-504
```

```
    DisableCMD: Unset

  Username: Guest
    SID: S-1-5-21-3043820608-1980768537-1953574876-501
    DisableCMD: Unset
```

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: 2024/08/14

Plugin Output

tcp/0

```
Device Name         : VirtualBox Graphics Adapter (WDDM)
Driver File Version : 7.0.8.6879
Driver Date         : 04/17/2023
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: 2024/08/14

Plugin Output

tcp/0

```
Windows accounts enumerated. Results output to DB.
User data gathered in scan starting at : 2024/8/21 6:49 AEST
```

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: 2022/05/25

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 3 NetBIOS names have been gathered :

 DC               = Computer name
 DC               = File Server Service
 WORKGROUP        = Workgroup / Domain name

The remote host has the following MAC address on its adapter :

   08:00:27:aa:5f:7a
```

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: 2024/08/14

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            : 10.0.20348.2520
  Supported Platform : Windows x64

  Path               : C:\Windows\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.20348.2520
  Supported Platform : Windows NT x86

--- Microsoft Print To PDF ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_9aa65d011441bcbc\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_9aa65d011441bcbc\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-VMK7H

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: 2024/08/14

Plugin Output

tcp/445/cifs

```
  -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: 2024/08/14

Plugin Output

tcp/0

```
Total : 347

  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 [...]
```