4- Windows10 Scan

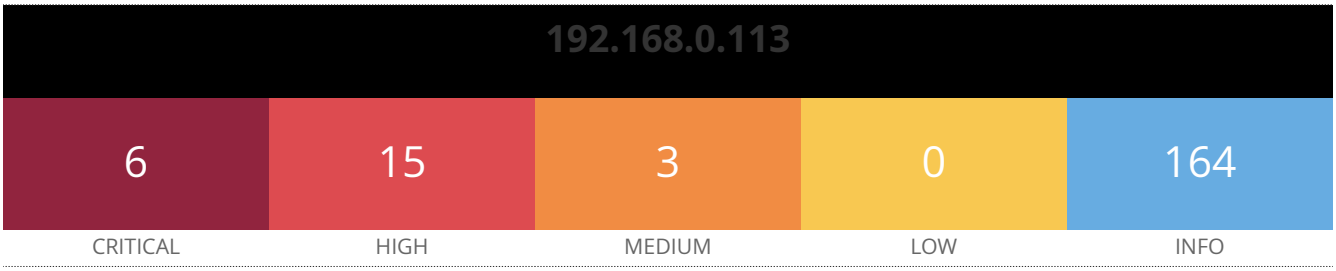
Report generated by Nessus™ Sun, 28 Aug 2022 14:56:49 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.113..... 4

Vulnerabilities by Host



Scan Information

Start time: Sun Aug 28 13:51:06 2022
End time: Sun Aug 28 14:55:59 2022

Host Information

Netbios Name: DESKTOP-AU88VVK
IP: 192.168.0.113
MAC Address: 58:FB:84:D7:C7:D3 00:0C:29:B2:FD:E8
OS: Microsoft Windows 10 Home

Vulnerabilities

156065 - KB5008212: Windows 10 Version 2004 / Windows 10 Version 20H2 / Windows 10 Version 21H1 / Windows 10 Version 21H2 Security Update (December 2021)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5008212.

It is, therefore, affected by multiple vulnerabilities:

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

(CVE-2021-41333, CVE-2021-43207, CVE-2021-43223, CVE-2021-43226, CVE-2021-43229, CVE-2021-43230, CVE-2021-43231, CVE-2021-43237, CVE-2021-43238, CVE-2021-43239, CVE-2021-43240, CVE-2021-43247, CVE-2021-43248, CVE-2021-43883, CVE-2021-43893)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-43215, CVE-2021-43217, CVE-2021-43232, CVE-2021-43233, CVE-2021-43234)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-43216, CVE-2021-43222, CVE-2021-43224, CVE-2021-43227, CVE-2021-43235, CVE-2021-43236, CVE-2021-43244)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-43219, CVE-2021-43228, CVE-2021-43246)

See Also

https://support.microsoft.com/en-us/help/5008212

Solution

Apply Cumulative Update KB5008212.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-41333
CVE	CVE-2021-43207
CVE	CVE-2021-43215
CVE	CVE-2021-43216
CVE	CVE-2021-43217
CVE	CVE-2021-43219
CVE	CVE-2021-43222
CVE	CVE-2021-43223
CVE	CVE-2021-43224
CVE	CVE-2021-43226
CVE	CVE-2021-43227

CVE	CVE-2021-43228
CVE	CVE-2021-43229
CVE	CVE-2021-43230
CVE	CVE-2021-43231
CVE	CVE-2021-43232
CVE	CVE-2021-43233
CVE	CVE-2021-43234
CVE	CVE-2021-43235
CVE	CVE-2021-43236
CVE	CVE-2021-43237
CVE	CVE-2021-43238
CVE	CVE-2021-43239
CVE	CVE-2021-43240
CVE	CVE-2021-43244
CVE	CVE-2021-43246
CVE	CVE-2021-43247
CVE	CVE-2021-43248
CVE	CVE-2021-43883
CVE	CVE-2021-43893
MSKB	5008212
XREF	MSFT:MS21-5008212
XREF	IAVA:2021-A-0586-S
XREF	IAVA:2021-A-0582-S

Plugin Information

Published: 2021/12/14, Modified: 2022/01/14

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5008212

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1415
```

156617 - KB5009543: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (January 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5009543.

It is, therefore, affected by multiple vulnerabilities:

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21849, CVE-2022-21850, CVE-2022-21851, CVE-2022-21874, CVE-2022-21878, CVE-2022-21892, CVE-2022-21893, CVE-2022-21922, CVE-2022-21928, CVE-2022-21958, CVE-2022-21959, CVE-2022-21960, CVE-2022-21961, CVE-2022-21962, CVE-2022-21963)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21876, CVE-2022-21880, CVE-2022-21904, CVE-2022-21915)

- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.

(CVE-2022-21894, CVE-2022-21900, CVE-2022-21905, CVE-2022-21913, CVE-2022-21924, CVE-2022-21925)

- A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2022-21836)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21843, CVE-2022-21848, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890)

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

(CVE-2022-21833, CVE-2022-21834, CVE-2022-21835, CVE-2022-21838, CVE-2022-21857, CVE-2022-21859, CVE-2022-21860, CVE-2022-21862, CVE-2022-21863, CVE-2022-21864, CVE-2022-21866, CVE-2022-21867, CVE-2022-21868, CVE-2022-21870, CVE-2022-21871, CVE-2022-21873, CVE-2022-21875, CVE-2022-21879, CVE-2022-21881, CVE-2022-21884, CVE-2022-21885, CVE-2022-21895, CVE-2022-21897, CVE-2022-21901, CVE-2022-21902, CVE-2022-21903, CVE-2022-21908, CVE-2022-21910, CVE-2022-21914, CVE-2022-21916, CVE-2022-21919, CVE-2022-21920)

See Also

https://support.microsoft.com/en-us/help/5009543

Solution

Apply Cumulative Update KB5009543.

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)

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-2021-22947
CVE	CVE-2021-36976
CVE	CVE-2022-21833
CVE	CVE-2022-21834
CVE	CVE-2022-21835
CVE	CVE-2022-21836
CVE	CVE-2022-21838
CVE	CVE-2022-21843
CVE	CVE-2022-21847
CVE	CVE-2022-21848
CVE	CVE-2022-21849
CVE	CVE-2022-21850
CVE	CVE-2022-21851
CVE	CVE-2022-21852
CVE	CVE-2022-21857
CVE	CVE-2022-21858
CVE	CVE-2022-21859
CVE	CVE-2022-21860
CVE	CVE-2022-21861
CVE	CVE-2022-21862
CVE	CVE-2022-21863
CVE	CVE-2022-21864
CVE	CVE-2022-21865
CVE	CVE-2022-21866
CVE	CVE-2022-21867
CVE	CVE-2022-21868

CVE	CVE-2022-21869
CVE	CVE-2022-21870
CVE	CVE-2022-21871
CVE	CVE-2022-21872
CVE	CVE-2022-21873
CVE	CVE-2022-21874
CVE	CVE-2022-21875
CVE	CVE-2022-21876
CVE	CVE-2022-21877
CVE	CVE-2022-21878
CVE	CVE-2022-21879
CVE	CVE-2022-21880
CVE	CVE-2022-21881
CVE	CVE-2022-21882
CVE	CVE-2022-21883
CVE	CVE-2022-21884
CVE	CVE-2022-21885
CVE	CVE-2022-21888
CVE	CVE-2022-21889
CVE	CVE-2022-21890
CVE	CVE-2022-21892
CVE	CVE-2022-21893
CVE	CVE-2022-21894
CVE	CVE-2022-21895
CVE	CVE-2022-21896
CVE	CVE-2022-21897
CVE	CVE-2022-21898
CVE	CVE-2022-21900
CVE	CVE-2022-21901
CVE	CVE-2022-21902
CVE	CVE-2022-21904
CVE	CVE-2022-21905
CVE	CVE-2022-21906
CVE	CVE-2022-21907
CVE	CVE-2022-21908
CVE	CVE-2022-21910
CVE	CVE-2022-21912
CVE	CVE-2022-21913
CVE	CVE-2022-21914
CVE	CVE-2022-21915
CVE	CVE-2022-21916
CVE	CVE-2022-21918
CVE	CVE-2022-21919

CVE	CVE-2022-21920
CVE	CVE-2022-21921
CVE	CVE-2022-21922
CVE	CVE-2022-21924
CVE	CVE-2022-21925
CVE	CVE-2022-21928
CVE	CVE-2022-21958
CVE	CVE-2022-21959
CVE	CVE-2022-21960
CVE	CVE-2022-21961
CVE	CVE-2022-21962
CVE	CVE-2022-21963
MSKB	5009543
XREF	MSFT:MS22-5009543
XREF	IAVA:2022-A-0012-S
XREF	IAVA:2022-A-0016-S
XREF	CISA-KNOWN-EXPLOITED:2022/02/18
XREF	CISA-KNOWN-EXPLOITED:2022/05/16

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/01/11, Modified: 2022/07/26

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5009543

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1466
```

159685 - KB5012599: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (April 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5012591.

It is, therefore, affected by multiple vulnerabilities:

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

(CVE-2022-26789, CVE-2022-26786, CVE-2022-26802, CVE-2022-26803, CVE-2022-26801, CVE-2022-26796, CVE-2022-26787, CVE-2022-26797, CVE-2022-26827, CVE-2022-26810, CVE-2022-26808, CVE-2022-26798, CVE-2022-24549, CVE-2022-26795, CVE-2022-26791, CVE-2022-26794, CVE-2022-26904, CVE-2022-26792, CVE-2022-26807, CVE-2022-26788, CVE-2022-26828, CVE-2022-26790, CVE-2022-26914, CVE-2022-26793, CVE-2022-24496, CVE-2022-24544, CVE-2022-24540, CVE-2022-24489, CVE-2022-24488, CVE-2022-24486, CVE-2022-24481, CVE-2022-24479, CVE-2022-24527, CVE-2022-24474, CVE-2022-24521, CVE-2022-24550, CVE-2022-24499, CVE-2022-24547, CVE-2022-24546, CVE-2022-24494, CVE-2022-24542, CVE-2022-24530)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-26831, CVE-2022-26915, CVE-2022-24538, CVE-2022-24484, CVE-2022-26784)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-26917, CVE-2022-26916, CVE-2022-26812, CVE-2022-26811, CVE-2022-26919, CVE-2022-26823, CVE-2022-26809, CVE-2022-26824, CVE-2022-26818, CVE-2022-26815, CVE-2022-26814, CVE-2022-26822, CVE-2022-26918, CVE-2022-26829, CVE-2022-26820, CVE-2022-26826, CVE-2022-26819, CVE-2022-26825, CVE-2022-26817, CVE-2022-26821, CVE-2022-26813, CVE-2022-24545, CVE-2022-24541, CVE-2022-24492, CVE-2022-24491, CVE-2022-24537, CVE-2022-24536, CVE-2022-24487, CVE-2022-24534, CVE-2022-24485, CVE-2022-24533, CVE-2022-26903, CVE-2022-24495, CVE-2022-24528, CVE-2022-23257, CVE-2022-21983, CVE-2022-22009, CVE-2022-22008, CVE-2022-24500)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-26816, CVE-2022-26920, CVE-2022-24493, CVE-2022-24539, CVE-2022-24490, CVE-2022-26783, CVE-2022-26785, CVE-2022-24498, CVE-2022-24483)

See Also

https://support.microsoft.com/en-us/help/5012591

Solution

Apply Security Update 5012599

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)

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-2022-21983
CVE	CVE-2022-22008
CVE	CVE-2022-22009
CVE	CVE-2022-23257
CVE	CVE-2022-24474
CVE	CVE-2022-24479
CVE	CVE-2022-24481
CVE	CVE-2022-24482
CVE	CVE-2022-24483
CVE	CVE-2022-24484
CVE	CVE-2022-24485
CVE	CVE-2022-24486
CVE	CVE-2022-24487
CVE	CVE-2022-24488
CVE	CVE-2022-24489
CVE	CVE-2022-24490
CVE	CVE-2022-24491
CVE	CVE-2022-24492
CVE	CVE-2022-24493
CVE	CVE-2022-24494
CVE	CVE-2022-24495
CVE	CVE-2022-24496
CVE	CVE-2022-24497
CVE	CVE-2022-24498
CVE	CVE-2022-24499
CVE	CVE-2022-24500

CVE	CVE-2022-24521
CVE	CVE-2022-24527
CVE	CVE-2022-24528
CVE	CVE-2022-24530
CVE	CVE-2022-24533
CVE	CVE-2022-24534
CVE	CVE-2022-24536
CVE	CVE-2022-24537
CVE	CVE-2022-24538
CVE	CVE-2022-24539
CVE	CVE-2022-24540
CVE	CVE-2022-24541
CVE	CVE-2022-24542
CVE	CVE-2022-24544
CVE	CVE-2022-24545
CVE	CVE-2022-24546
CVE	CVE-2022-24547
CVE	CVE-2022-24549
CVE	CVE-2022-24550
CVE	CVE-2022-26783
CVE	CVE-2022-26784
CVE	CVE-2022-26785
CVE	CVE-2022-26786
CVE	CVE-2022-26787
CVE	CVE-2022-26788
CVE	CVE-2022-26789
CVE	CVE-2022-26790
CVE	CVE-2022-26791
CVE	CVE-2022-26792
CVE	CVE-2022-26793
CVE	CVE-2022-26794
CVE	CVE-2022-26795
CVE	CVE-2022-26796
CVE	CVE-2022-26797
CVE	CVE-2022-26798
CVE	CVE-2022-26801
CVE	CVE-2022-26802
CVE	CVE-2022-26803
CVE	CVE-2022-26807
CVE	CVE-2022-26808
CVE	CVE-2022-26809
CVE	CVE-2022-26810
CVE	CVE-2022-26811

CVE	CVE-2022-26812
CVE	CVE-2022-26813
CVE	CVE-2022-26814
CVE	CVE-2022-26815
CVE	CVE-2022-26816
CVE	CVE-2022-26817
CVE	CVE-2022-26818
CVE	CVE-2022-26819
CVE	CVE-2022-26820
CVE	CVE-2022-26821
CVE	CVE-2022-26822
CVE	CVE-2022-26823
CVE	CVE-2022-26824
CVE	CVE-2022-26825
CVE	CVE-2022-26826
CVE	CVE-2022-26827
CVE	CVE-2022-26828
CVE	CVE-2022-26829
CVE	CVE-2022-26831
CVE	CVE-2022-26903
CVE	CVE-2022-26904
CVE	CVE-2022-26914
CVE	CVE-2022-26915
CVE	CVE-2022-26916
CVE	CVE-2022-26917
CVE	CVE-2022-26918
CVE	CVE-2022-26919
CVE	CVE-2022-26920
MSKB	5012599
XREF	MSFT:MS22-5012599
XREF	IAVA:2022-A-0147-S
XREF	IAVA:2022-A-0145-S
XREF	CISA-KNOWN-EXPLOITED:2022/05/04
XREF	CISA-KNOWN-EXPLOITED:2022/05/16

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/04/12, Modified: 2022/07/26

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5012599

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1645
```

160927 - KB5013942: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (May 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5013942. It is, therefore, affected by multiple vulnerabilities

- Windows LDAP Remote Code Execution Vulnerability (CVE-2022-22012, CVE-2022-22013, CVE-2022-22014, CVE-2022-29128, CVE-2022-29129, CVE-2022-29130, CVE-2022-29131, CVE-2022-29137, CVE-2022-29139, CVE-2022-29141)

- Windows Network File System Remote Code Execution Vulnerability (CVE-2022-26937)

- Windows Graphics Component Remote Code Execution Vulnerability (CVE-2022-26927)

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/5013942

Solution

Apply Security Update 5013942

Risk Factor

High

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)

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

I

References

CVE	CVE-2022-21972
CVE	CVE-2022-22011
CVE	CVE-2022-22012
CVE	CVE-2022-22013
CVE	CVE-2022-22014
CVE	CVE-2022-22015
CVE	CVE-2022-22016
CVE	CVE-2022-22019
CVE	CVE-2022-22713
CVE	CVE-2022-23270
CVE	CVE-2022-23279
CVE	CVE-2022-24466
CVE	CVE-2022-26913
CVE	CVE-2022-26923
CVE	CVE-2022-26925
CVE	CVE-2022-26926
CVE	CVE-2022-26927
CVE	CVE-2022-26930
CVE	CVE-2022-26931
CVE	CVE-2022-26932
CVE	CVE-2022-26933
CVE	CVE-2022-26934
CVE	CVE-2022-26935
CVE	CVE-2022-26936
CVE	CVE-2022-26937
CVE	CVE-2022-26938
CVE	CVE-2022-26939
CVE	CVE-2022-29102
CVE	CVE-2022-29103
CVE	CVE-2022-29104
CVE	CVE-2022-29105
CVE	CVE-2022-29106
CVE	CVE-2022-29112
CVE	CVE-2022-29113
CVE	CVE-2022-29114
CVE	CVE-2022-29115
CVE	CVE-2022-29120
CVE	CVE-2022-29121

CVE	CVE-2022-29122
CVE	CVE-2022-29123
CVE	CVE-2022-29125
CVE	CVE-2022-29126
CVE	CVE-2022-29127
CVE	CVE-2022-29128
CVE	CVE-2022-29129
CVE	CVE-2022-29130
CVE	CVE-2022-29131
CVE	CVE-2022-29132
CVE	CVE-2022-29134
CVE	CVE-2022-29135
CVE	CVE-2022-29137
CVE	CVE-2022-29138
CVE	CVE-2022-29139
CVE	CVE-2022-29140
CVE	CVE-2022-29141
CVE	CVE-2022-29142
CVE	CVE-2022-29150
CVE	CVE-2022-29151
CVE	CVE-2022-30138
MSKB	5013942
XREF	MSFT:MS22-5013942
XREF	IAVA:2022-A-0204-S
XREF	IAVA:2022-A-0203-S
XREF	CISA-KNOWN-EXPLOITED:2022/07/22
XREF	CISA-KNOWN-EXPLOITED:2022/09/08

Plugin Information

Published: 2022/05/10, Modified: 2022/08/19

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5013942

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1706
```

163951 - KB5016616: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (August 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5016616. It is, therefore, affected by multiple vulnerabilities

- Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability (CVE-2022-35747, CVE-2022-35769)

- Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability (CVE-2022-30133, CVE-2022-35744)

- Windows Bluetooth Service Remote Code Execution Vulnerability (CVE-2022-30144)

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/en-us/help/5016616

https://support.microsoft.com/help/5016616

Solution

Apply Security Update 5016616

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-30133
CVE	CVE-2022-30144
CVE	CVE-2022-30194
CVE	CVE-2022-30197
CVE	CVE-2022-33670
CVE	CVE-2022-34301
CVE	CVE-2022-34302
CVE	CVE-2022-34303
CVE	CVE-2022-34690
CVE	CVE-2022-34691
CVE	CVE-2022-34696
CVE	CVE-2022-34699
CVE	CVE-2022-34701
CVE	CVE-2022-34702
CVE	CVE-2022-34703
CVE	CVE-2022-34704
CVE	CVE-2022-34705
CVE	CVE-2022-34706
CVE	CVE-2022-34707
CVE	CVE-2022-34708
CVE	CVE-2022-34709
CVE	CVE-2022-34710
CVE	CVE-2022-34712
CVE	CVE-2022-34713
CVE	CVE-2022-34714
CVE	CVE-2022-35743
CVE	CVE-2022-35744
CVE	CVE-2022-35745
CVE	CVE-2022-35746
CVE	CVE-2022-35747
CVE	CVE-2022-35748
CVE	CVE-2022-35749
CVE	CVE-2022-35750
CVE	CVE-2022-35751
CVE	CVE-2022-35752
CVE	CVE-2022-35753
CVE	CVE-2022-35754
CVE	CVE-2022-35755

CVE	CVE-2022-35756
CVE	CVE-2022-35757
CVE	CVE-2022-35758
CVE	CVE-2022-35759
CVE	CVE-2022-35760
CVE	CVE-2022-35761
CVE	CVE-2022-35762
CVE	CVE-2022-35763
CVE	CVE-2022-35764
CVE	CVE-2022-35765
CVE	CVE-2022-35766
CVE	CVE-2022-35767
CVE	CVE-2022-35768
CVE	CVE-2022-35769
CVE	CVE-2022-35771
CVE	CVE-2022-35792
CVE	CVE-2022-35793
CVE	CVE-2022-35794
CVE	CVE-2022-35795
CVE	CVE-2022-35797
CVE	CVE-2022-35820
MSKB	5016616
XREF	MSFT:MS22-5016616
XREF	CISA-KNOWN-EXPLOITED:2022/08/30
XREF	IAVA:2022-A-0319
XREF	IAVA:2022-A-0320

Plugin Information

Published: 2022/08/09, Modified: 2022/08/15

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5016616

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1889
```

22024 - Microsoft Internet Explorer Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of Internet Explorer.

Description

According to its self-reported version number, the installation of Microsoft Internet Explorer on the remote Windows host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://www.nessus.org/u?9802ce93

http://www.nessus.org/u?e0d2ff5a

https://docs.microsoft.com/en-us/deployedge/edge-ie-disable-ie11

Solution

Either Upgrade to a version of Internet Explorer that is currently supported or disable Internet Explorer on the target device.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0557

Plugin Information

Published: 2006/07/11, Modified: 2022/06/28

Plugin Output

tcp/445/cifs

```
The remote host has Internet Explorer version 11.789.19041.0 installed, which is no longer
 supported.

Internet Explorer is being detected as enabled on this device.
This is due to the fact that the Registry key is missing or not set:

'\HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\NotifyDisableIEOptions'
```

157429 - KB5010342: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (February 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5010342. It is, therefore, affected by multiple vulnerabilities

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21993, CVE-2022-21998)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-22002)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21992, CVE-2022-21995)

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

(CVE-2022-21989, CVE-2022-21994, CVE-2022-21997, CVE-2022-21999, CVE-2022-22000, CVE-2022-22001)

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://support.microsoft.com/en-us/help/5010342

Solution

Apply Security Update 5010342

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

I

References

CVE	CVE-2022-21971
CVE	CVE-2022-21974
CVE	CVE-2022-21981
CVE	CVE-2022-21984
CVE	CVE-2022-21985
CVE	CVE-2022-21989
CVE	CVE-2022-21992
CVE	CVE-2022-21993
CVE	CVE-2022-21994
CVE	CVE-2022-21995
CVE	CVE-2022-21997
CVE	CVE-2022-21998
CVE	CVE-2022-21999
CVE	CVE-2022-22000
CVE	CVE-2022-22001
CVE	CVE-2022-22002
CVE	CVE-2022-22710
CVE	CVE-2022-22712
CVE	CVE-2022-22715
CVE	CVE-2022-22717
CVE	CVE-2022-22718
MSKB	5010342
XREF	MSFT:MS22-5010342
XREF	IAVA:2022-A-0074-S
XREF	IAVA:2022-A-0068-S
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/05/10
XREF	CISA-KNOWN-EXPLOITED:2022/09/08

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/02/08, Modified: 2022/08/19

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5010342

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1526
```

158701 - KB5011487: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (March 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5011487. It is, therefore, affected by multiple vulnerabilities:

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

(CVE-2022-23283, CVE-2022-23284, CVE-2022-23291, CVE-2022-24459, CVE-2022-23296, CVE-2022-24507, CVE-2022-24454, CVE-2022-23298, CVE-2022-23290, CVE-2022-23288, CVE-2022-24525, CVE-2022-24460, CVE-2022-23299, CVE-2022-23293, CVE-2022-23287, CVE-2022-21967, CVE-2022-24505, CVE-2022-23286)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21975, CVE-2022-23253)

- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.

(CVE-2022-24502)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21977, CVE-2022-22010, CVE-2022-23281, CVE-2022-23297, CVE-2022-24503)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21990, CVE-2022-23285, CVE-2022-23294, CVE-2022-24508)

See Also

https://support.microsoft.com/en-us/help/5011487

Solution

Apply Security Update 5011487.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-21967
CVE	CVE-2022-21975
CVE	CVE-2022-21977
CVE	CVE-2022-21990
CVE	CVE-2022-22010
CVE	CVE-2022-23253
CVE	CVE-2022-23278
CVE	CVE-2022-23281
CVE	CVE-2022-23283
CVE	CVE-2022-23284
CVE	CVE-2022-23285
CVE	CVE-2022-23286
CVE	CVE-2022-23287
CVE	CVE-2022-23288
CVE	CVE-2022-23290
CVE	CVE-2022-23291
CVE	CVE-2022-23293
CVE	CVE-2022-23294
CVE	CVE-2022-23296
CVE	CVE-2022-23297
CVE	CVE-2022-23298
CVE	CVE-2022-23299
CVE	CVE-2022-24454
CVE	CVE-2022-24459
CVE	CVE-2022-24460
CVE	CVE-2022-24502
CVE	CVE-2022-24503
CVE	CVE-2022-24505
CVE	CVE-2022-24507
CVE	CVE-2022-24508
CVE	CVE-2022-24525
MSKB	5011487
XREF	MSFT:MS22-5011487

XREF IAVA:2022-A-0111-S
XREF IAVA:2022-A-0112-S

Plugin Information

Published: 2022/03/08, Modified: 2022/07/26

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5011487

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1586
```

162201 - KB5014699: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (June 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5014699. It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-30166, CVE-2022-30165, CVE-2022-30160 CVE-2022-30154, CVE-2022-30151, CVE-2022-30150, CVE-2022-30147, CVE-2022-30132, CVE-2022-30131)

- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application. (CVE-2022-30164)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-30163, CVE-2022-30161, CVE-2022-30153, CVE-2022-30149, CVE-2022-30146, CVE-2022-30145, CVE-2022-30143, CVE-2022-30142, CVE-2022-30141, CVE-2022-30140, CVE-2022-30139,CVE-2022-30190)

See Also

https://support.microsoft.com/help/5014699

Solution

Apply Security Update 5014699

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

I

References

CVE	CVE-2022-21123
CVE	CVE-2022-21125
CVE	CVE-2022-21127
CVE	CVE-2022-21166
CVE	CVE-2022-30132
CVE	CVE-2022-30139
CVE	CVE-2022-30140
CVE	CVE-2022-30141
CVE	CVE-2022-30142
CVE	CVE-2022-30143
CVE	CVE-2022-30145
CVE	CVE-2022-30146
CVE	CVE-2022-30147
CVE	CVE-2022-30148
CVE	CVE-2022-30149
CVE	CVE-2022-30150
CVE	CVE-2022-30151
CVE	CVE-2022-30152
CVE	CVE-2022-30153
CVE	CVE-2022-30155
CVE	CVE-2022-30160
CVE	CVE-2022-30161
CVE	CVE-2022-30162
CVE	CVE-2022-30163
CVE	CVE-2022-30164
CVE	CVE-2022-30165
CVE	CVE-2022-30166
CVE	CVE-2022-30189
CVE	CVE-2022-30190
CVE	CVE-2022-32230
MSKB	5014699
XREF	MSFT:MS22-5014699
XREF	IAVA:2022-A-0240-S
XREF	IAVA:2022-A-0241-S
XREF	CISA-KNOWN-EXPLOITED:2022/07/05

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/06/14, Modified: 2022/07/26

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5014699

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1766
```

163048 - KB5015807: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (July 2022)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5015807. It is, therefore, affected by multiple vulnerabilities:

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-22024, CVE-2022-22027, CVE-2022-22029, CVE-2022-22038, CVE-2022-22039, CVE-2022-30211, CVE-2022-30214, CVE-2022-30221, CVE-2022-30222)

- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.

(CVE-2022-22023, CVE-2022-22048, CVE-2022-30203)

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

(CVE-2022-22022, CVE-2022-22026, CVE-2022-22031, CVE-2022-22034, CVE-2022-22036, CVE-2022-22037, CVE-2022-22041, CVE-2022-22045, CVE-2022-22047, CVE-2022-22049, CVE-2022-22050, CVE-2022-30202, CVE-2022-30205, CVE-2022-30206, CVE-2022-30209, CVE-2022-30215, CVE-2022-30220, CVE-2022-30224, CVE-2022-30225, CVE-2022-30226)

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/en-us/help/5015807

https://support.microsoft.com/help/5015807

Solution

Apply Security Update 5015807

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-21845
CVE	CVE-2022-22022
CVE	CVE-2022-22023
CVE	CVE-2022-22024
CVE	CVE-2022-22025
CVE	CVE-2022-22026
CVE	CVE-2022-22027
CVE	CVE-2022-22028
CVE	CVE-2022-22029
CVE	CVE-2022-22031
CVE	CVE-2022-22034
CVE	CVE-2022-22036
CVE	CVE-2022-22037
CVE	CVE-2022-22038
CVE	CVE-2022-22039
CVE	CVE-2022-22040
CVE	CVE-2022-22041
CVE	CVE-2022-22042
CVE	CVE-2022-22043
CVE	CVE-2022-22045
CVE	CVE-2022-22047
CVE	CVE-2022-22048
CVE	CVE-2022-22049
CVE	CVE-2022-22050
CVE	CVE-2022-22711
CVE	CVE-2022-27776
CVE	CVE-2022-30202
CVE	CVE-2022-30203
CVE	CVE-2022-30205
CVE	CVE-2022-30206
CVE	CVE-2022-30208

CVE	CVE-2022-30209
CVE	CVE-2022-30211
CVE	CVE-2022-30212
CVE	CVE-2022-30213
CVE	CVE-2022-30214
CVE	CVE-2022-30215
CVE	CVE-2022-30216
CVE	CVE-2022-30220
CVE	CVE-2022-30221
CVE	CVE-2022-30222
CVE	CVE-2022-30223
CVE	CVE-2022-30224
CVE	CVE-2022-30225
CVE	CVE-2022-30226
CVE	CVE-2022-33644
MSKB	5015807
XREF	MSFT:MS22-5015807
XREF	CISA-KNOWN-EXPLOITED:2022/08/02
XREF	IAVA:2022-A-0272-S
XREF	IAVA:2022-A-0273-S

Plugin Information

Published: 2022/07/12, Modified: 2022/08/22

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5015807

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.1288
    Should be      : 10.0.19041.1826
```

141430 - Microsoft 3D Viewer Base3D Code Execution (October 2020)

Synopsis

The Windows app installed on the remote host is affected by a code execution vulnerability.

Description

The Microsoft 3D Viewer app installed on the remote host is affected by a code execution vulnerability when the Base3D rendering engine improperly handles memory. An attacker who successfully exploited the vulnerability would gain execution on a victim system.

See Also

http://www.nessus.org/u?4a0fa39f

http://www.nessus.org/u?baf22b1a

https://www.zerodayinitiative.com/advisories/ZDI-20-1246/

Solution

Upgrade to app version 7.2009.29132.0 or later via the Microsoft Store.

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)

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)

References

CVE	CVE-2020-16918
CVE	CVE-2020-17003
XREF	ZDI:ZDI-20-1246

Plugin Information

Published: 2020/10/13, Modified: 2020/11/24

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2009.29132.0
```

150352 - Microsoft 3D Viewer Multiple Vulnerabilities (June 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilties.

Description

The Windows '3D Viewer' app installed on the remote host is affected by multiple vulnerabilities.

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-31942, CVE-2021-31943)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-31944)

See Also

http://www.nessus.org/u?e914ff80

http://www.nessus.org/u?5257edc0

http://www.nessus.org/u?bdd18cf9

Solution

Upgrade to app version 7.2105.4012.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-31942

CVE	CVE-2021-31943
CVE	CVE-2021-31944

Plugin Information

Published: 2021/06/08, Modified: 2021/06/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2105.4012.0
```

154988 - Microsoft 3D Viewer Multiple Vulnerabilities (November 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilities.

Description

The version of the Microsoft 3D Viewer app installed on the remote host is prior to 7.2107.7012.0. It is, therefore, affected by multiple remote code execution vulnerabilities.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43208

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43209

Solution

Upgrade to app version 7.2107.7012.0., or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-43208
CVE	CVE-2021-43209

Plugin Information

Published: 2021/11/09, Modified: 2021/11/18

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2107.7012.0
```

158710 - Microsoft Paint 3D Code Execution (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a code execution vulnerability..

Description

The Windows 'Paint 3D' app installed on the remote host is affected by a code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23282

Solution

Upgrade to app version 6.2105.4017.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-23282

Plugin Information

Published: 2022/03/08, Modified: 2022/03/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MSPaint_6.1907.29027.0_x64__8wekyb3d8bbwe
  Installed version : 6.1907.29027.0
  Fixed version     : 6.2105.4017.0
```

158708 - Microsoft Windows HEIF Image Extensions RCE (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows HEIF Image Extension app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24457

Solution

Upgrade to app version 1.0.43012.0 or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-24457

Plugin Information

Published: 2022/03/08, Modified: 2022/03/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.HEIFImageExtension_1.0.22742.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22742.0
  Fixed version     : 1.0.43012.0
```

158706 - Microsoft Windows VP9 Video Extensions Library Multiple Vulnerabilities (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a multiple code execution vulnerabilities.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by multiple code execution vulnerabilities. An attacker who successfully exploited the vulnerabilities could execute arbitrary code. Exploitation of the vulnerabilities require that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24451

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-24451
CVE	CVE-2022-24501

Plugin Information

Published: 2022/03/08, Modified: 2022/03/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

148484 - Microsoft Windows VP9 Video Extensions Library RCE (April 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?4bb22046

Solution

Upgrade to app version 1.0.40631.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-28464

Plugin Information

Published: 2021/04/13, Modified: 2021/04/13

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.40631.0
```

157438 - Microsoft Windows VP9 Video Extensions Library RCE (February 2022)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?0c177c5b

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-22709

Plugin Information

Published: 2022/02/08, Modified: 2022/02/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

150355 - Microsoft Windows VP9 Video Extensions Library RCE (June 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?af8af611

Solution

Upgrade to app version 1.0.41182.0, or later via the Microsoft Store.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-31967

Plugin Information

Published: 2021/06/08, Modified: 2021/06/14

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.41182.0
```

149388 - Microsoft Windows Web Media Extensions Library RCE (May 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'Web Media Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file. (CVE-2021-28465)

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28465

Solution

Upgrade to app version 1.0.40831.0, or later via the Microsoft Store.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-28465

Plugin Information

Published: 2021/05/11, Modified: 2021/05/12

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.WebMediaExtensions_1.0.20875.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.20875.0
  Fixed version     : 1.0.40831.0
```

140596 - Microsoft Windows WebP Image Extension RCE (August 2020)

Synopsis

The Windows app installed on the remote host is affected by a Remote Code Execution Vulnerability.

Description

The Windows 'WebP Image Extension' or 'WebP from Device Manufacturer' app installed on the remote host is affected by a remote code execution vulnerability.

An unauthenticated, remote attacker can exploit this vulnerability via an specially crafted image to execute code and gain control of the system.

See Also

http://www.nessus.org/u?f2638e5b

Solution

Upgrade to app version 1.0.31251.0 or later via the Microsoft Store.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-1574

XREF IAVA:2020-A-0361-S

Plugin Information

Published: 2020/09/15, Modified: 2022/08/26

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.WebpImageExtension_1.0.22753.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22753.0
  Fixed version     : 1.0.31251.0
```

150373 - Microsoft Paint 3D Multiple Vulnerabilities (June 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilities.

Description

The Windows 'Paint 3D' app installed on the remote host is affected by multiple remote code execution vulnerabilities. An attacker can exploit these to bypass authentication and execute unauthorized arbitrary commands.

See Also

http://www.nessus.org/u?941966fe

http://www.nessus.org/u?a40919a7

http://www.nessus.org/u?99b641c8

Solution

Upgrade to app version 6.2105.4017.0, or later via the Microsoft Store.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-31945
CVE	CVE-2021-31946
CVE	CVE-2021-31983

Plugin Information

Published: 2021/06/08, Modified: 2021/06/11

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MSPaint_6.1907.29027.0_x64__8wekyb3d8bbwe
  Installed version : 6.1907.29027.0
  Fixed version     : 6.2105.4017.0
```

158205 - Microsoft Windows VP9 Video Extensions Library Information Disclosure (December 2021)

Synopsis

The Windows app installed on the remote host is affected by an information disclosure vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by an information disclosure vulnerability.

An authenticated, local attacker can exploit this, to disclose potentially sensitive information.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43243

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-43243

Plugin Information

Published: 2022/02/21, Modified: 2022/02/22

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

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: 2021/03/15

Plugin Output

tcp/445/cifs

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: 2022/02/01

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\4.18.2205.7-0\
  Version                      : 4.18.2205.7
  Engine version               : 1.1.19500.2
  Antivirus signature version  : 1.373.1100.0
  Antispyware signature version : 1.373.1100.0
```

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.
```

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: 2022/08/15

Plugin Output

tcp/0

```
Vendor       : VMware, Inc.
Version      : VMW71.00V.14410784.B64.1908150010
Release date : 20190815000000.000000+000
UUID         : FC274D56-BBD9-B53D-E568-E5F680B2FDE8
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: 2022/08/22

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_10:::x64-home -> Microsoft Windows 10 64-bit

Following application CPE's matched on the remote system :

  cpe:/a:microsoft:.net_framework:4.8 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:104.0.1293.70 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.789.19041.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:remote_desktop_connection:10.0.19041.1266 -> Microsoft Remote Desktop Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.2205.7 -> Microsoft System Center Endpoint
 Protection
  cpe:/a:microsoft:windows_defender:4.18.2205.7 -> Microsoft Windows Defender
```

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: 2022/08/15

Plugin Output

tcp/0

```
Computer Manufacturer : VMware, Inc.
Computer Model : VMware7,1
Computer SerialNumber : VMware-56 4d 27 fc d9 bb 3d b5-e5 68 e5 f6 80 b2 fd e8
Computer Type : Other

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

Computer Memory : 1022 MB
  RAM slot #0
    Form Factor: DIMM
    Type       : DRAM
    Capacity   : 1024 MB
```

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 : 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 : \\DESKTOP-AU88VVK

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 : \\DESKTOP-AU88VVK

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 : \\DESKTOP-AU88VVK

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

```
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\DESKTOP-AU88VVK

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
Named pipe : \pipe\eventlog
Netbios name : \\DESKTOP-AU88VVK

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\DESKTOP-AU88VVK

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\DESKTOP-AU88VVK

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Descri [...]
```

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 : 192.168.0.113

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 : 192.168.0.113

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 : 192.168.0.113

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 : 192.168.0.113
```

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 : 192.168.0.113
```

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 : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.0.113

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

```
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.0.113
```

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 : 192.168.0.113

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 : 192.168.0.113

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
```

```
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.0.113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description :  [...]
```

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 : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.0.113

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 : 49668
IP : 192.168.0.113

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 : 49668
IP : 192.168.0.113

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 : 49668
IP : 192.168.0.113

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 : 49668
IP : 192.168.0.113
```

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 : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.0.113
```

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/49670/dce-rpc

```
The following DCERPC services are available on TCP port 49670 :

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 : 49670
IP : 192.168.0.113
```

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: 2022/08/15

Plugin Output

tcp/445/cifs

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

Package      : Microsoft-OneCore-ApplicationModel-Sync-Desktop-FOD-
Package~31bf3856ad364e35~amd64~~10.0.19041.746
State        : Installed
Release Type : OnDemand Pack
Install Time : 10/6/2021 1:58 PM

Package      : Microsoft-OneCore-DirectX-Database-FOD-Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 12/7/2019 9:52 AM

Package      : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~10.0.19041.1266
State        : Installed
Release Type : Language Pack
Install Time : 10/6/2021 1:58 PM

Package      : Microsoft-Windows-FodMetadata-Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : Feature Pack
Install Time : 12/7/2019 9:49 AM

Package      : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~10.0.19041.1
```

```
State        : Installed
Release Type : Foundation
Install Time : 12/7/2019 9:18 AM

Package      : Microsoft-Windows-Hello-Face-Package~31bf3856ad364e35~amd64~~10.0.19041.1202
State        : Installed
Release Type : OnDemand Pack
Install Time : 10/6/2021 1:58 PM

Package      : Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~11.0.19041.1202
State        : Installed
Release Type : OnDemand Pack
Install Time : 10/6/2021 1:58 PM

Package      : Microsoft-Windows-LanguageFeatures-Basic-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 12/7/2019 9:51 AM

Package      : Microsoft-Windows-LanguageFeatures-Handwriting-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 12/7/2019 9:51 AM

Package      : Microsoft-Windows-LanguageFeatures-OCR-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 12/7/2019 9:51 AM

Package      : Microsoft-Windows-LanguageFeatures-Spe [...]
```

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: 2022/08/15

Plugin Output

tcp/0

```
Hostname : DESKTOP-AU88VVK
  DESKTOP-AU88VVK (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: 2011/05/23

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: 2022/08/15

Plugin Output

tcp/0

```
Group Name : Administrators
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-544
Members    :
  Name : Administrator
    Domain : DESKTOP-AU88VVK
    Class  : Win32_UserAccount
    SID    : S-1-5-21-772112266-2597022876-2739506520-500
  Name : padmi
    Domain : DESKTOP-AU88VVK
    Class  : Win32_UserAccount
    SID    : S-1-5-21-772112266-2597022876-2739506520-1001

Group Name : Device Owners
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-583
Members    :

Group Name : Distributed COM Users
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-562
Members    :

Group Name : Event Log Readers
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-573
Members    :

Group Name : Guests
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-546
Members    :
```

```
  Name : Guest
    Domain : DESKTOP-AU88VVK
    Class  : Win32_UserAccount
    SID    : S-1-5-21-772112266-2597022876-2739506520-501

Group Name : Hyper-V Administrators
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-578
Members    :

Group Name : IIS_IUSRS
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-568
Members    :
  Name : IUSR
    Domain : DESKTOP-AU88VVK
    Class  : Win32_SystemAccount
    SID    : S-1-5-17

Group Name : Performance Log Users
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-559
Members    :

Group Name : Performance Monitor Users
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-558
Members    :

Group Name : Remote Management Users
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-580
Members    :

Group Name : System Managed Accounts Group
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-581
Members    :
  Name : DefaultAccount
    Domain : DESKTOP-AU88VVK
    Class  : Win32_UserAccount
    SID    : S-1-5-21-772112266-2597022876-2739506520-503

Group Name : Users
Host Name  : DESKTOP-AU88VVK
Group SID  : S-1-5-32-545
Members    :
  Name : INTERACTIVE
    Domain : DESKTOP-AU88VVK
    Class  : Win32_SystemAccount
    SID    : S-1-5-4
  Name : Authenticated Users
    Domain : DESKTOP-AU88VVK
    Class  : Win32_SystemAc [...]
```

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: 2022/08/15

Plugin Output

tcp/0

```
Name            : Administrator
SID             : S-1-5-21-772112266-2597022876-2739506520-500
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : DefaultAccount
SID             : S-1-5-21-772112266-2597022876-2739506520-503
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Guest
SID             : S-1-5-21-772112266-2597022876-2739506520-501
Disabled        : True
Lockout         : False
Change password : False
Source          : Local

Name            : padmi
SID             : S-1-5-21-772112266-2597022876-2739506520-1001
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : WDAGUtilityAccount
```

```
SID             : S-1-5-21-772112266-2597022876-2739506520-504
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

No. Of Users : 5
```

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 :

58:FB:84:D7:C7:D3 : Intel Corporate
00:0C:29:B2:FD:E8 : VMware, Inc.
```

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:
  - 58:FB:84:D7:C7:D3
  - 00:0C:29:B2:FD:E8
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.0.113 resolves as DESKTOP-AU88VVK.
```

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

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is 1 second.
```

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://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/

Solution

n/a

Risk Factor

None

Plugin Information

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

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.
```

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: 2022/05/25

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\pushtoinstall.dll,-200 : Windows PushToInstall Service
@%systemroot%\system32\ci.dll,-100 : Isolated User Mode (IUM)
@%systemroot%\system32\sysmain.dll,-1000 : SysMain
@%systemroot%\system32\captureservice.dll,-100 : CaptureService
c:\windows\system32,@elscore.dll,-5 : Microsoft Transliteration Engine
@%systemroot%\system32\dosvc.dll,-100 : Delivery Optimization
@%programfiles%\windows defender\mpasdesc.dll,-370 : Microsoft Defender Antivirus Network Inspection
 System Driver
c:\windows\system32,@elscore.dll,-1 : Microsoft Language Detection
@%systemroot%\system32\userdataaccessres.dll,-10003 : User Data Storage
@%systemroot%\system32\appxdeploymentserver.dll,-1 : AppX Deployment Service (AppXSVC)
@%systemroot%\system32\windows.devices.picker.dll,-1006 : DevicePicker
@%systemroot%\system32\tokenbroker.dll,-100 : Web Account Manager
@winlangdb.dll,-1121 : English (United States)
@%systemroot%\system32\userdataaccessres.dll,-15001 : Contact Data
@%systemroot%\system32\wpnservice.dll,-1 : Windows Push Notifications System Service
@%systemroot%\system32\dnsapi.dll,-103 : Domain Name System (DNS) Server Trust
@%systemroot%\system32\credentialenrollmentmanager.exe,-100 : CredentialEnrollmentManagerUserSvc
@%systemroot%\system32\vaultsvc.dll,-1003 : Credential Manager
c:\windows\system32,@elscore.dll,-3 : Microsoft Traditional Chinese to Simplified Chinese
 Transliteration
c:\windows\system32,@elscore.dll,-8 : Microsoft Malayalam to Latin Transliteration
```

```
@%systemroot%\system32\cdpusersvc.dll,-100 : Connected Devices Platform User Service
@%systemroot%\system32\ngcsvc.dll,-100 : Microsoft Passport
@%systemroot%\system32\searchindexer.exe,-103 : Windows Search
@%systemroot%\system32\wuaueng.dll,-105 : Windows Update
@%systemroot%\system32\sgrmbroker.exe,-100 : System Guard Runtime Monitor Broker
@%systemroot%\system32\moshost.dll,-100 : Downloaded Maps Manager
@%systemroot%\system32\fveui.dll,-844 : BitLocker Data Recovery Agent
@%systemroot%\servicing\trustedinstaller.exe,-100 : Windows Modules Instal [...]
```

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: 2022/02/01

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 : 4.8.04084
  Install Type : Full
  Release      : 528372

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.04084
  Install Type : Client
  Release      : 528372
```

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: 2022/08/22

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 104.0.1293.70
```

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: 2022/08/22

Plugin Output

tcp/0

```
Path    : C:\Windows\system32\mshtml.dll
Version : 11.0.19041.1288
```

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  : 11.789.19041.0
```

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: 2019/11/22

Plugin Output

tcp/0

```
Path    : C:\Windows\\System32\\mstsc.exe
Version : 10.0.19041.1266
```

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 :

  - DESKTOP-AU88VVK\Administrator (User)
  - DESKTOP-AU88VVK\padmi (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 accounts have been disabled :

  - 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.
```

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 users have never changed their passwords :\n
  - 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.
```

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 user has a password that never expires :

  - padmi


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: 2022/08/15

Plugin Output

tcp/0

```
192.168.0.1 : b4-75-0e-ad-03-dc
192.168.0.107 : 58-fb-84-d7-c7-d3
192.168.0.255 : 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: 2022/08/15

Plugin Output

tcp/0

```
    fe3cr.delivery.mp.microsoft.com
    fe3cr.delivery.mp.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 : 6
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 2
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 4c04
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : Intel64 Family 6 Model 76 Stepping 4, GenuineIntel
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-772112266-2597022876-2739506520-1001
    onedrive : C:\Users\padmi\OneDrive
    temp : %USERPROFILE%\AppData\Local\Temp
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
```

```
    tmp : %USERPROFILE%\AppData\Local\Temp
    onedriveconsumer : C:\Users\padmi\OneDrive
```

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
```

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 :

Microsoft Edge  [version 104.0.1293.70]  [installed on 2022/08/27]
Microsoft Edge Update  [version 1.3.167.21]
Microsoft Update Health Tools  [version 3.67.0.0]  [installed on 2022/08/28]
```

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 : 2022-08-28T13:49:49+05:30 (20220828134949.500000+330)
```

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-1-5-21-772112266-2597022876-2739506520-1001
    Domain   : DESKTOP-AU88VVK
    Username : padmi
```

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\d:
  Data     : \??\SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD01#5&2edf08dd&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004e00450043005600 4d00570061007200260005

  Name     : \??\volume{459f42f5-26fd-11ed-8c8f-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD01#5&2edf08dd&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004e00450043005600 4d00570061007200260005

  Name     : \dosdevices\c:
  Data     : DMIO:ID:=%)8MY
  Raw data : 444d494f3a49443a3d25ce29aa38d24da11dcfd3dc59f0f0
```

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: 2022/08/15

Plugin Output

tcp/0

```
NBT information attached.
First 10 lines of all CSVs:
nbtstat_local.csv:
Interface,Name,Suffix,Type,Status,MAC
192.168.0.113,DESKTOP-AU88VVK,<00>,UNIQUE,Registered,00:0C:29:B2:FD:E8
192.168.0.113,WORKGROUP,<00>,GROUP,Registered,00:0C:29:B2:FD:E8
192.168.0.113,DESKTOP-AU88VVK,<20>,UNIQUE,Registered,00:0C:29:B2:FD:E8
192.168.0.113,WORKGROUP,<1E>,GROUP,Registered,00:0C:29:B2:FD:E8
192.168.0.113,WORKGROUP,<1D>,UNIQUE,Registered,00:0C:29:B2:FD:E8
192.168.0.113,..__MSBROWSE__.,<01>,GROUP,Registered,00:0C:29:B2:FD:E8
```

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) 82574L Gigabit Network Connection
Network Adapter Driver Version     : 12.17.10.8
```

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

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: 2022/08/15

Plugin Output

tcp/0

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- Memory Compression (1700)
 0 :    |- smss.exe (328)
 1 : explorer.exe (3196)
 1 : |- SecurityHealthSystray.exe (1856)
 1 : |- OneDrive.exe (5208)
 0 : csrss.exe (412)
 0 : wininit.exe (488)
 0 : |- services.exe (620)
 0 :    |- svchost.exe (1048)
 0 :    |- svchost.exe (1284)
 0 :    |- svchost.exe (1296)
 0 :    |- svchost.exe (1304)
 0 :    |- spoolsv.exe (1344)
 0 :    |- svchost.exe (1556)
 0 :    |- svchost.exe (1668)
 0 :    |- svchost.exe (1772)
 0 :       |- audiodg.exe (5864)
 0 :    |- svchost.exe (1820)
 0 :    |- svchost.exe (1976)
 0 :    |- svchost.exe (2008)
 0 :    |- svchost.exe (2228)
 0 :    |- svchost.exe (2348)
 0 :    |- MsMpEng.exe (2452)
 0 :    |- svchost.exe (2704)
```

```
1 :    |- svchost.exe (2976)
0 :    |- svchost.exe (3360)
1 :    |- svchost.exe (3568)
0 :    |- svchost.exe (360)
1 :       |- taskhostw.exe (2248)
1 :       |- sihost.exe (2912)
0 :       |- WMIADAP.exe (3520)
0 :    |- SearchIndexer.exe (4060)
0 :       |- SearchFilterHost.exe (1324)
0 :       |- SearchProtocolHost.exe (5812)
0 :    |- NisSrv.exe (424)
0 :    |- svchost.exe (4700)
0 :    |- SecurityHealthService.exe (5152)
0 :    |- SgrmBroker.exe (6048)
0 :    |- svchost.exe (680)
0 :    |- svchost.exe (748)
1 :       |- SearchApp.exe (2292)
1 :       |- RuntimeBroker.exe (372)
1 :       |- StartMenuExperienceHost.exe (4044)
1 :       |- RuntimeBroker.exe (4192)
1 :       |- backgroundTaskHost.exe (4240)
1 :       |- ShellExperienceHost.exe (4424)
0 :       |- WmiPrvSE.exe (4560)
1 :       |- SkypeApp.exe (4604)
1 :       |- SettingSyncHost.exe (4672)
1 :       |- SkypeBackgroundHost.exe (4684)
0 :       |- MoUsoCoreWorker.exe (4920)
0 :          |- wuauclt.exe (4488)
1 :       |- smartscreen.exe (5128)
1 :       |- RuntimeBroker.exe (5160)
0 :       |- TiWorker.exe (5232)
1 :       |- RuntimeBroker.exe (5884)
0 :       |- WmiPrvSE.exe (6 [...]
```

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: 2022/08/15

Plugin Output

tcp/0

```
Process_Modules_192.168.0.113.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: 2022/08/15

Plugin Output

tcp/135/epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 932).

This process 'svchost.exe' (pid 932) 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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

Plugin Output

udp/500

```
The Win32 process 'svchost.exe' is listening on this port (pid 360).

This process 'svchost.exe' (pid 360) is hosting the following Windows services :
Browser (@%systemroot%\system32\browser.dll,-100)
gpsvc (@gpapi.dll,-112)
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
iphlpsvc (@%SystemRoot%\system32\iphlpsvc.dll,-500)
LanmanServer (@%systemroot%\system32\srvsvc.dll,-100)
ProfSvc (@%systemroot%\system32\profsvc.dll,-300)
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
SENS (@%SystemRoot%\system32\Sens.dll,-200)
ShellHWDetection (@%SystemRoot%\System32\shsvcs.dll,-12288)
Themes (@%SystemRoot%\System32\themeservice.dll,-8192)
TokenBroker (@%systemroot%\system32\tokenbroker.dll,-100)
UserManager (@%systemroot%\system32\usermgr.dll,-100)
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
wlidsvc (@%SystemRoot%\system32\wlidsvc.dll,-100)
WpnService (@%SystemRoot%\system32\wpnservice.dll,-1)
wuauserv (@%systemroot%\system32\wuaueng.dll,-105)
```

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: 2022/08/15

Plugin Output

udp/1900

```
The Win32 process 'svchost.exe' is listening on this port (pid 1284).

This process 'svchost.exe' (pid 1284) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
SensrSvc (@%SystemRoot%\System32\sensrsvc.dll,-1000)
SSDPSRV (@%systemroot%\system32\ssdpsrv.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: 2022/08/15

Plugin Output

udp/3702

```
The Win32 process 'svchost.exe' is listening on this port (pid 1284).

This process 'svchost.exe' (pid 1284) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
SensrSvc (@%SystemRoot%\System32\sensrsvc.dll,-1000)
SSDPSRV (@%systemroot%\system32\ssdpsrv.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: 2022/08/15

Plugin Output

udp/4500

```
The Win32 process 'svchost.exe' is listening on this port (pid 360).

This process 'svchost.exe' (pid 360) is hosting the following Windows services :
Browser (@%systemroot%\system32\browser.dll,-100)
gpsvc (@gpapi.dll,-112)
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
iphlpsvc (@%SystemRoot%\system32\iphlpsvc.dll,-500)
LanmanServer (@%systemroot%\system32\srvsvc.dll,-100)
ProfSvc (@%systemroot%\system32\profsvc.dll,-300)
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
SENS (@%SystemRoot%\system32\Sens.dll,-200)
ShellHWDetection (@%SystemRoot%\System32\shsvcs.dll,-12288)
Themes (@%SystemRoot%\System32\themeservice.dll,-8192)
TokenBroker (@%systemroot%\system32\tokenbroker.dll,-100)
UserManager (@%systemroot%\system32\usermgr.dll,-100)
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
wlidsvc (@%SystemRoot%\system32\wlidsvc.dll,-100)
WpnService (@%SystemRoot%\system32\wpnservice.dll,-1)
wuauserv (@%systemroot%\system32\wuaueng.dll,-105)
```

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: 2022/08/15

Plugin Output

tcp/5040

```
The Win32 process 'svchost.exe' is listening on this port (pid 1304).

This process 'svchost.exe' (pid 1304) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
DispBrokerDesktopSvc (@%SystemRoot%\system32\dispbroker.desktop.dll,-101)
EventSystem (@comres.dll,-2450)
fdPHost (@%systemroot%\system32\fdPHost.dll,-100)
FontCache (@%systemroot%\system32\FntCache.dll,-100)
LicenseManager (@%SystemRoot%\system32\licensemanagersvc.dll,-200)
netprofm (@%SystemRoot%\system32\netprofmsvc.dll,-202)
nsi (@%SystemRoot%\system32\nsisvc.dll,-200)
RemoteRegistry (Remote Registry)
WdiServiceHost (@%systemroot%\system32\wdi.dll,-502)
```

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: 2022/08/15

Plugin Output

udp/5050

```
The Win32 process 'svchost.exe' is listening on this port (pid 1304).

This process 'svchost.exe' (pid 1304) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
DispBrokerDesktopSvc (@%SystemRoot%\system32\dispbroker.desktop.dll,-101)
EventSystem (@comres.dll,-2450)
fdPHost (@%systemroot%\system32\fdPHost.dll,-100)
FontCache (@%systemroot%\system32\FntCache.dll,-100)
LicenseManager (@%SystemRoot%\system32\licensemanagersvc.dll,-200)
netprofm (@%SystemRoot%\system32\netprofmsvc.dll,-202)
nsi (@%SystemRoot%\system32\nsisvc.dll,-200)
RemoteRegistry (Remote Registry)
WdiServiceHost (@%systemroot%\system32\wdi.dll,-502)
```

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: 2022/08/15

Plugin Output

udp/5353

```
The Win32 process 'svchost.exe' is listening on this port (pid 1556).

This process 'svchost.exe' (pid 1556) is hosting the following Windows services :
CryptSvc (@%SystemRoot%\system32\cryptsvc.dll,-1001)
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
LanmanWorkstation (@%systemroot%\system32\wkssvc.dll,-100)
NlaSvc (@%SystemRoot%\System32\nlasvc.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: 2022/08/15

Plugin Output

udp/5355

```
The Win32 process 'svchost.exe' is listening on this port (pid 1556).

This process 'svchost.exe' (pid 1556) is hosting the following Windows services :
CryptSvc (@%SystemRoot%\system32\cryptsvc.dll,-1001)
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
LanmanWorkstation (@%systemroot%\system32\wkssvc.dll,-100)
NlaSvc (@%SystemRoot%\System32\nlasvc.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: 2022/08/15

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: 2022/08/15

Plugin Output

tcp/49664/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 640).

This process 'lsass.exe' (pid 640) is hosting the following Windows services :
KeyIso (@keyiso.dll,-100)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
VaultSvc (@%SystemRoot%\system32\vaultsvc.dll,-1003)
```

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: 2022/08/15

Plugin Output

tcp/49665/dce-rpc

```
The Win32 process 'wininit.exe' is listening on this port (pid 488).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2022/08/15

Plugin Output

tcp/49666/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 680).

This process 'svchost.exe' (pid 680) is hosting the following Windows services :
Dhcp (@%SystemRoot%\system32\dhcpcore.dll,-100)
EventLog (@%SystemRoot%\system32\wevtsvc.dll,-200)
lmhosts (@%SystemRoot%\system32\lmhsvc.dll,-101)
NgcCtnrSvc (@%SystemRoot%\System32\NgcCtnrSvc.dll,-1)
TimeBrokerSvc (@%windir%\system32\TimeBrokerServer.dll,-1001)
WinHttpAutoProxySvc (@%SystemRoot%\system32\winhttp.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: 2022/08/15

Plugin Output

tcp/49667/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 360).

This process 'svchost.exe' (pid 360) is hosting the following Windows services :
Browser (@%systemroot%\system32\browser.dll,-100)
gpsvc (@gpapi.dll,-112)
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
iphlpsvc (@%SystemRoot%\system32\iphlpsvc.dll,-500)
LanmanServer (@%systemroot%\system32\srvsvc.dll,-100)
ProfSvc (@%systemroot%\system32\profsvc.dll,-300)
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
SENS (@%SystemRoot%\system32\Sens.dll,-200)
ShellHWDetection (@%SystemRoot%\System32\shsvcs.dll,-12288)
Themes (@%SystemRoot%\System32\themeservice.dll,-8192)
TokenBroker (@%systemroot%\system32\tokenbroker.dll,-100)
UserManager (@%systemroot%\system32\usermgr.dll,-100)
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
wlidsvc (@%SystemRoot%\system32\wlidsvc.dll,-100)
WpnService (@%SystemRoot%\system32\wpnservice.dll,-1)
wuauserv (@%systemroot%\system32\wuaueng.dll,-105)
```

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: 2022/08/15

Plugin Output

tcp/49668/dce-rpc

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 1344).

This process 'spoolsv.exe' (pid 1344) 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: 2022/08/15

Plugin Output

tcp/49669/dce-rpc

```
The Win32 process 'services.exe' is listening on this port (pid 620).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2022/08/15

Plugin Output

tcp/49670/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 2228).

This process 'svchost.exe' (pid 2228) 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: 2022/08/15

Plugin Output

udp/55491

```
The Win32 process 'svchost.exe' is listening on this port (pid 1284).

This process 'svchost.exe' (pid 1284) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
SensrSvc (@%SystemRoot%\System32\sensrsvc.dll,-1000)
SSDPSRV (@%systemroot%\system32\ssdpsrv.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: 2022/08/15

Plugin Output

udp/55496

```
The Win32 process 'svchost.exe' is listening on this port (pid 1284).

This process 'svchost.exe' (pid 1284) is hosting the following Windows services :
FDResPub (@%systemroot%\system32\fdrespub.dll,-100)
SensrSvc (@%SystemRoot%\System32\sensrsvc.dll,-1000)
SSDPSRV (@%systemroot%\system32\ssdpsrv.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: 2022/08/15

Plugin Output

udp/55498

```
The Win32 process 'dasHost.exe' is listening on this port (pid 2356).
```

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: Disabled
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 : .\padmi
```

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: 2021/07/27

Plugin Output

tcp/445/cifs

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

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: 2019/10/04

Plugin Output

tcp/445/cifs

```
The remote host SID value is :

1-5-21-772112266-2597022876-2739506520

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: DESKTOP-AU88VVK
NetBIOS Domain Name: DESKTOP-AU88VVK
NetBIOS Computer Name: DESKTOP-AU88VVK
DNS Domain Name: DESKTOP-AU88VVK
DNS Computer Name: DESKTOP-AU88VVK
DNS Tree Name: unknown
Product Version: 10.0.19041
```

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 = 10.19044
Architecture = x64
Build lab extended = 19041.1.amd64fre.vb_release.191206-1406
```

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 :

  AudioEndpointBuilder startup parameters :
    Display name : Windows Audio Endpoint Builder
    Service name : AudioEndpointBuilder
    Log on as : LocalSystem
    Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p

  Audiosrv startup parameters :
    Display name : Windows Audio
    Service name : Audiosrv
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
    Dependencies : AudioEndpointBuilder/RpcSs/

  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_33cae startup parameters :
    Display name : Connected Devices Platform User Service_33cae
    Service name : CDPUserSvc_33cae
    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  [...]
```

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 :

AppX Deployment Service (AppXSVC) [ AppXSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Computer Browser [ Browser ]
Connected Devices Platform Service [ CDPSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Association Service [ DeviceAssociationService ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
Display Enhancement Service [ DisplayEnhancementService ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Data Usage [ DusmSvc ]
```

```
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Function Discovery Provider Host [ fdPHost ]
Function Discovery Resource Publication [ FDResPub ]
Windows Font Cache Service [ FontCache ]
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 ]
Network Connection Broker [ NcbService ]
Network Connected Devices Auto-Setup [ NcdAutoSetup ]
Network List Service [ netprofm ]
Microsoft Passport Container [ NgcCtnrSvc ]
Microsoft Passport [ NgcSvc ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
Remote Registry [ RemoteRegistry ]
Radio Management Service [ RmSvc ]
RPC Endpoint Mapper [ RpcEptMapper ]
Remote Procedure Call (RPC) [ RpcSs ]
Security Accounts Manager [ SamSs ]
Task Scheduler [ Schedule ]
Windows Security Service [ SecurityHealthService ]
Payments and NFC/SE Manager [ SEMgrSvc ]
System Event Notification Service [...]
```

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: 2022/08/15

Plugin Output

tcp/0

```
padmi

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_10.0.19041.746_none_ebc47b06544bfaab\MsoIrmProtector.doc
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.746_none_f619255888acbca6\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_10.0.19041.746_none_ebc47b06544bfaab\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.746_none_f619255888acbca6\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_10.0.19041.746_none_ebc47b06544bfaab\MsoIrmProtector.xls
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.746_none_f619255888acbca6\MsoIrmProtector.xls
```

11777 - Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

Synopsis

The remote host may contain material (movies/audio) infringing copyright.

Description

This plugin displays a list of media files (such as .mp3, .ogg, .mpg, .avi) which have been found on the remote SMB shares.

Some of these files may contain copyrighted materials, such as commercial movies or music files, that are being shared without the owner's permission.

If any of these files actually contain copyrighted material, and if they are freely swapped around, your organization might be held liable for copyright infringement by associations such as the RIAA or the MPAA.

Solution

Delete the files infringing copyright.

Risk Factor

None

Plugin Information

Published: 2003/06/26, Modified: 2012/11/29

Plugin Output

tcp/445/cifs

```
Here is a list of files which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial
movies or music files.

 + C$ :

C:\Program Files\WindowsApps\Microsoft.XboxApp_48.49.31001.0_x64__8wekyb3d8bbwe\Assets
\AchievementUnlocked.mp3
C:\Program Files\WindowsApps\Microsoft.ZuneVideo_10.19071.19011.0_x64__8wekyb3d8bbwe\Assets
\ImmersiveControl_Slider_Click_Sound.wma
```

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 padmi :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
addins
appcompat
apppatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
CbsTemp
Containers
Core.xml
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
DtcInstall.log
ELAMBKUP
```

```
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IME
ImmersiveControlPanel
INF
InputMethod
Installer
L2Schemas
LanguageOverlayCache
LiveKernelReports
Logs
lsasetup.log
Media
mib.bin
Microsoft.NET
Migration
ModemLogs
notepad.exe
OCR
Offline Web Pages
Panther
Performance
PLA
PolicyDefinitions
Prefetch
PrintDialog
Provisioning
regedit.exe
Registration
rescache
Resources
SchCache
schemas
security
ServiceProfiles
ServiceState
servicing
Setup
ShellComponents
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
SystemResources
SysWOW64
TAPI
Tasks
Temp
tracing
twain_32
twain_32.dll
Vss
WaaS
Web
win.ini
WindowsShell.Manifest
WindowsUpdate.log
```

```
winhlp32.exe
WinSxS
WMSysPr9.prx

- C$  - (readable,writable)
  + Content of this share :
$WinREAgent
Documents and Settings
DumpStack.log.tmp
OneDriveTemp
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swapfile.sys
System Volume Information
Users
Windows
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host when logged in as padmi:

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

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.
```

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 :

  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
```

38153 - Microsoft Windows Summary of Missing Patches

Synopsis

The remote host is missing several Microsoft security patches.

Description

This plugin summarizes updates for Microsoft Security Bulletins or Knowledge Base (KB) security updates that have not been installed on the remote Windows host based on the results of either a credentialed check using the supplied credentials or a check done using a supported third-party patch management tool.

Note the results of missing patches also include superseded patches.

Review the summary and apply any missing updates in order to be up to date.

Solution

Run Windows Update on the remote host or use a patch management solution.

Risk Factor

None

Plugin Information

Published: 2009/04/24, Modified: 2019/06/13

Plugin Output

tcp/445/cifs

```
The patches for the following bulletins or KBs are missing on the remote host :

 - KB5008212 ( https://support.microsoft.com/en-us/help/5008212 )
 - KB5009543 ( https://support.microsoft.com/en-us/help/5009543 )
 - KB5010342 ( https://support.microsoft.com/en-us/help/5010342 )
 - KB5011487 ( https://support.microsoft.com/en-us/help/5011487 )
 - KB5012599 ( https://support.microsoft.com/en-us/help/5012599 )
 - KB5013942 ( https://support.microsoft.com/en-us/help/5013942 )
 - KB5014699 ( https://support.microsoft.com/en-us/help/5014699 )
 - KB5015807 ( https://support.microsoft.com/en-us/help/5015807 )
 - KB5016616 ( https://support.microsoft.com/en-us/help/5016616 )
```

92369 - Microsoft Windows Time Zone Information

Synopsis

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

Description

Nesssus 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: 2020/06/12

Plugin Output

tcp/0

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : India Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : India Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : India Daylight Time
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 : 0xFFFFFEB6
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0xFFFFFEB6
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: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202208280343
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : 4- Windows10 Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.107
Port scanner(s) : wmi_netstat
Port range : default
Ping RTT : 7.986 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as '192.168.0.113\padmi' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2022/8/28 13:51 India Standard Time
Scan duration : 3865 sec
```

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: 2021/09/16

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: 2022/08/15

Plugin Output

tcp/0

```
Nessus was able to find 27 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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

Plugin Output

udp/1900

```
Port 1900/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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

Plugin Output

tcp/5040

```
Port 5040/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: 2022/08/15

Plugin Output

udp/5050

```
Port 5050/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: 2022/08/15

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: 2022/08/15

Plugin Output

udp/5355

```
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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

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: 2022/08/15

Plugin Output

tcp/49670/dce-rpc

```
Port 49670/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: 2022/08/15

Plugin Output

udp/55491

```
Port 55491/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: 2022/08/15

Plugin Output

udp/55496

```
Port 55496/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: 2022/08/15

Plugin Output

udp/55498

```
Port 55498/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: 2022/08/15

Plugin Output

tcp/0

```
+ Network Interface Information :

 - Network Interface = [00000001] Intel(R) 82574L Gigabit Network Connection
 - MAC Address = 00:0C:29:B2:FD:E8
 - IPAddress/IPSubnet = 192.168.0.113/255.255.255.0
 - IPAddress/IPSubnet = fe80::680c:3f79:71ff:22cb/64
 - IPAddress/IPSubnet = fd73:145a:bdf:0:a8e4:66ce:f7b:23c7/128
 - IPAddress/IPSubnet = fd73:145a:bdf:0:680c:3f79:71ff:22cb/64


+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    0.0.0.0         0.0.0.0         192.168.0.1
    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
    192.168.0.0     255.255.255.0   0.0.0.0
    192.168.0.113   255.255.255.255 0.0.0.0
    192.168.0.255   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
    255.255.255.255 255.255.255.255 0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
```

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: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 10 Home
Confidence level : 100
Method : SMB_OS

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-HTTPAPI/2.0

SinFP:!:
   P1:B11113:F0x12:W65392:O0204ffff:M1460:
   P2:B11113:F0x12:W65535:O0204ffff0103030801010402:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190300_7_p=49665


The remote host is running Microsoft Windows 10 Home
```

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  : 192.168.0.113\padmi
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: 2022/08/15

Plugin Output

tcp/0

```
. You need to take the following action :
+ Install the following Microsoft patch :

- KB5016616 (8 vulnerabilities)
```

92428 - Recent File History

Synopsis

Nessus was able to enumerate recently opened files on the remote host.

Description

Nessus was able to gather evidence of files opened by file type from the remote host.

See Also

https://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
C:\\Users\padmi\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-1-5-18
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1000
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1001
C:\\$Recycle.Bin\\S-1-5-18\.
C:\\$Recycle.Bin\\S-1-5-18\..
C:\\$Recycle.Bin\\S-1-5-18\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1000\.
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1000\..
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1000\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1001\.
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1001\..
C:\\$Recycle.Bin\\S-1-5-21-772112266-2597022876-2739506520-1001\desktop.ini
```

92430 - Registry Editor Last Accessed

Synopsis

Nessus was able to find the last key accessed by the Registry Editor when it was closed on the remote host.

Description

Nessus was able to find evidence of the last key that was opened when the Registry Editor was closed for each user.

See Also

https://support.microsoft.com/en-us/help/244004

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
padmi
  - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

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 :

KB5003791, Installed on: 2021/10/06
KB5004331, Installed on: 2021/10/06
KB5005699, Installed on: 2021/10/06
KB5010472, Installed on: 2022/08/28
KB5015895, Installed on: 2022/08/28
KB5016592, Installed on: 2022/08/28
```

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: 2019/07/08

Plugin Output

tcp/445/cifs

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - padmi (id 1001)

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.
```

97086 - Server Message Block (SMB) Protocol Version 1 Enabled

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

Plugin Information

Published: 2017/02/09, Modified: 2020/06/12

Plugin Output

tcp/445/cifs

```
SMBv1 client is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10\Start : 2
```

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: 2022/07/26

Plugin Output

tcp/5357/www

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

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: 2021/07/26

Plugin Output

tcp/445/cifs

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

User:       '192.168.0.113\padmi'
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: 2021/07/26

Plugin Output

tcp/445/cifs

```
Nessus was able to log in to the remote host via the following :

User:       '192.168.0.113\padmi'
Port:       445
Proto:      SMB
Method:     password
```

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

```
20220828134949.500000+330
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.107 to 192.168.0.113 :
192.168.0.107
192.168.0.113

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\padmi\Downloads\desktop.ini
C:\\Users\padmi\Downloads\Firefox Setup 3.6.12.exe
C:\\Users\Public\Downloads\desktop.ini

Download folder content report attached.
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

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.skydrive.desktop
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
microsoft.windows.controlpanel
microsoft.getstarted_8wekyb3d8bbwe!app
microsoft.windowscalculator_8wekyb3d8bbwe!app
microsoft.people_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x
c:\users\padmi\downloads\firefox setup 3.6.12.exe
microsoft.windowsfeedbackhub_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\services.msc
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\file explorer.lnk
microsoft.windows.search_cw5n1h2txyewy!cortanaui
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!app
microsoft.windows.shell.rundialog
c:\users\padmi\appdata\local\temp\~nsu.tmp\au_.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\services.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\wf.msc
microsoft.microsoftstickynotes_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\useraccountcontrolsettings.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\paint.lnk
microsoft.xboxgamingoverlay_8wekyb3d8bbwe!app
ueme_ctlcuacount:ctor
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\microsoft edge.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\cmd.exe
{f38bf404-1d43-42f2-9305-67de0b28fc23}\regedit.exe
```

```
msedge
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\snippingtool.exe
microsoft.windows.explorer
microsoft.windowsmaps_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\mspaint.exe
ueme_ctlsession
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\registry editor.lnk
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\snipping tool.lnk
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\mozilla firefox\firefox.exe

Extended userassist report attached.
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

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: 2022/08/15

Plugin Output

tcp/445/cifs

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

Microsoft Windows 10 Home
```

51187 - WMI Encryptable Volume Enumeration

Synopsis

The remote Windows host has encryptable volumes available.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates encryptable volume information available on the remote host via WMI.

See Also

http://www.nessus.org/u?8aa7973e

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/12/15, Modified: 2022/08/15

Plugin Output

tcp/0

```
Here is a list of encryptable volumes available on the remote system :

+ DriveLetter C:

  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{29ce253d-38aa-4dd2-a11d-cfd3dc59f0f0}\
  - Encryption Method : None
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - Protection Status : Protection Off
  - Size : 59.39 GB
```

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: 2022/08/15

Plugin Output

tcp/0

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

+ KB5016592
  - Description : Update
  - InstalledOn : 8/28/2022

+ KB5003791
  - Description : Update
  - InstalledOn : 10/6/2021

+ KB5006670
  - Description : Security Update
  - InstalledOn : 10/6/2021

+ KB5015895
  - Description : Update
  - InstalledOn : 8/28/2022

+ KB5005699
  - Description : Security Update
  - InstalledOn : 10/6/2021
```

```
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'.
```

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-1-5-21-772112266-2597022876-2739506520-1001
```

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: 2022/08/15

Plugin Output

tcp/0

```
+ Computer System Product
  - IdentifyingNumber : VMware-56 4d 27 fc d9 bb 3d b5-e5 68 e5 f6 80 b2 fd e8
  - Description       : Computer System Product
  - Vendor            : VMware, Inc.
  - Name              : VMware7,1
  - UUID              : FC274D56-BBD9-B53D-E568-E5F680B2FDE8
  - Version           : None
```

159817 - Windows Credential Guard Status

Synopsis

Windows Credential Guard is disabled on the remote Windows host.

Description

Windows Credential Guard is disabled on the remote Windows host.

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

Enable Credential Guard per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/04/18, Modified: 2022/04/25

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: Default
DhcpNameServer: 49.205.72.130 183.82.243.66 192.168.0.1
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/15, Modified: 2022/08/22

Plugin Output

tcp/0

```
Path                          : C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2205.7-0\
Version                       : 4.18.2205.7
Engine Version                : 1.1.19500.2
Malware Signature Timestamp : Aug. 28, 2022 at 02:56:53 GMT
Malware Signature Version   : 1.373.1100.0
Signatures Last Updated     : Aug. 28, 2022 at 07:51:25 GMT
```

72482 - Windows Display Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the display drivers on the remote host.

Description

Nessus was able to enumerate one or more of the display drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?b6e87533

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0756

Plugin Information

Published: 2014/02/06, Modified: 2022/08/15

Plugin Output

tcp/0

```
Device Name         : Microsoft Basic Display Adapter
Driver File Version : 10.0.19041.868
Driver Date         : 06/21/2006
Video Processor     : VMware
```

92423 - Windows Explorer Recently Executed Programs

Synopsis

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

Description

Nessus was able to find evidence of program execution using Windows Explorer registry logs and settings.

See Also

http://www.forensicswiki.org/wiki/LastVisitedMRU

http://www.nessus.org/u?7e00b191

http://www.nessus.org/u?ac4dd3fb

http://www.nessus.org/u?c409cb41

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2019/08/15

Plugin Output

tcp/0

```
mspaint\1
ba
cmd\1

 MRU programs details in attached report.
```

159929 - Windows LSA Protection Status

Synopsis

Windows LSA Protection is disabled on the remote Windows host.

Description

The LSA Protection validates users for local and remote sign-ins and enforces local security policies to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protects against Pass-the-Hash or Mimikatz-style attacks.

Solution

Enable LSA Protection per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/04/20, Modified: 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 6 NetBIOS names have been gathered :

 DESKTOP-AU88VVK  = Computer name
 WORKGROUP        = Workgroup / Domain name
 DESKTOP-AU88VVK  = File Server Service
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

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

   00:0c:29:b2:fd:e8
```

77668 - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot% \prefetch*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?8242d04f

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/09/12, Modified: 2018/11/15

Plugin Output

tcp/0

```
+ HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3

+ Prefetch file list :
  - \Windows\prefetch\AM_BASE.EXE-3F70DC95.pf
  - \Windows\prefetch\AM_DELTA.EXE-78CA83B0.pf
  - \Windows\prefetch\AM_ENGINE.EXE-F1C956E4.pf
  - \Windows\prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf
  - \Windows\prefetch\ARP.EXE-ED14DF84.pf
  - \Windows\prefetch\AUDIODG.EXE-AB22E9A6.pf
  - \Windows\prefetch\AU_.EXE-4AA74771.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-031D5A98.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-05A8BF9D.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-09FABB87.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-3803E50A.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-7165C35C.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-743B8179.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-772AFF02.pf
```

```
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-07EA5F06.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-621DBAF8.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-887DD0F8.pf
  - \Windows\prefetch\BYTECODEGENERATOR.EXE-FB938A53.pf
  - \Windows\prefetch\CLOUDEXPERIENCEHOSTBROKER.EXE-AB26EBC7.pf
  - \Windows\prefetch\CMD.EXE-0BD30981.pf
  - \Windows\prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf
  - \Windows\prefetch\CONHOST.EXE-0C6456FB.pf
  - \Windows\prefetch\CONSENT.EXE-40419367.pf
  - \Windows\prefetch\CREDENTIALENROLLMENTMANAGER.E-856B6153.pf
  - \Windows\prefetch\CREDENTIALUIBROKER.EXE-8CEDA3EB.pf
  - \Windows\prefetch\CSRSS.EXE-F3C368CB.pf
  - \Windows\prefetch\CTFMON.EXE-795F8130.pf
  - \Windows\prefetch\DASHOST.EXE-4B84F273.pf
  - \Windows\prefetch\DEFRAG.EXE-3D9E8D72.pf
  - \Windows\prefetch\DISM.EXE-AA0F2086.pf
  - \Windows\prefetch\DISMHOST.EXE-22CAC53B.pf
  - \Windows\prefetch\DISMHOST.EXE-553AC8C9.pf
  - \Windows\prefetch\DISMHOST.EXE-98C500DF.pf
  - \Windows\prefetch\DISMHOST.EXE-A10EA93E.pf
  - \Windows\prefetch\DLLHOST.EXE-15CDDA9C.pf
  - \Windows\prefetch\DLLHOST.EXE-3D723117.pf
  - \Windows\prefetch\DLLHOST.EXE-4427C062.pf
  - \W [...]
```

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: 2022/08/22

Plugin Output

tcp/445/cifs

```
--- Microsoft Shared Fax Driver ---

  Path               : C:\Windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL
  Version            : 10.0.19041.1023
  Supported Platform : Windows x64

--- 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            : 10.0.19041.1202
  Supported Platform : Windows x64

  Path               : C:\Windows\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.19041.906
  Supported Platform : Windows NT x86

--- Microsoft Print To PDF ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_c62e9f8067f98247\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.1
  Supported Platform : Windows x64
```

```
--- Microsoft Software Printer Driver ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_c62e9f8067f98247\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.1
  Supported Platform : Windows x64

--- Microsoft XPS Document Writer v4 ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_c62e9f8067f98247\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.1
  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-8HVX7

Note that all but the final portion of the key has been obfuscated.
```

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: 2022/08/22

Plugin Output

tcp/445/cifs

```
  -1527c705-839a-4832-9118-54d4Bd6a0c89
      Version : 10.0.19041.1023
      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 : 10.0.19041.1023
      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 : 10.0.19041.1023
      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 : 10.0.19041.1023
      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 : 1000.19041.1023.0
    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 : 10.0.19041.1023
    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 : 10.0.19041.1023
    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 : 10.0.1 [...]
```