Qualys. Community Edition

Scan Results

September 23, 2024

Report Summary	
User Name:	Jacob Brown
Login Name:	hckry3ab
Company:	Hickory Computer
User Role:	Manager
Address:	
City:	Hickory
State:	North Carolina
Zip:	28601
Country:	United States of America
Created:	09/23/2024 at 12:13:01 (GMT-0400)
Launch Date:	09/23/2024 at 12:03:55 (GMT-0400)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1727107435.97539
Scanner Appliances:	Testing (Scanner 12.18.33-1, Vulnerability Signatures 2.6.146-2)
Authentication:	Windows authentication was successful for 1 host
Duration:	00:04:52
Title:	Authenticated Scan 2
Asset Groups:	-
IPs:	10.0.0.197
Excluded IPs:	-
Options Profile:	Test Scan

Summary of Vulnerabilities

Vulnerabilities Total	300

Security Risk (Avg)	5.0

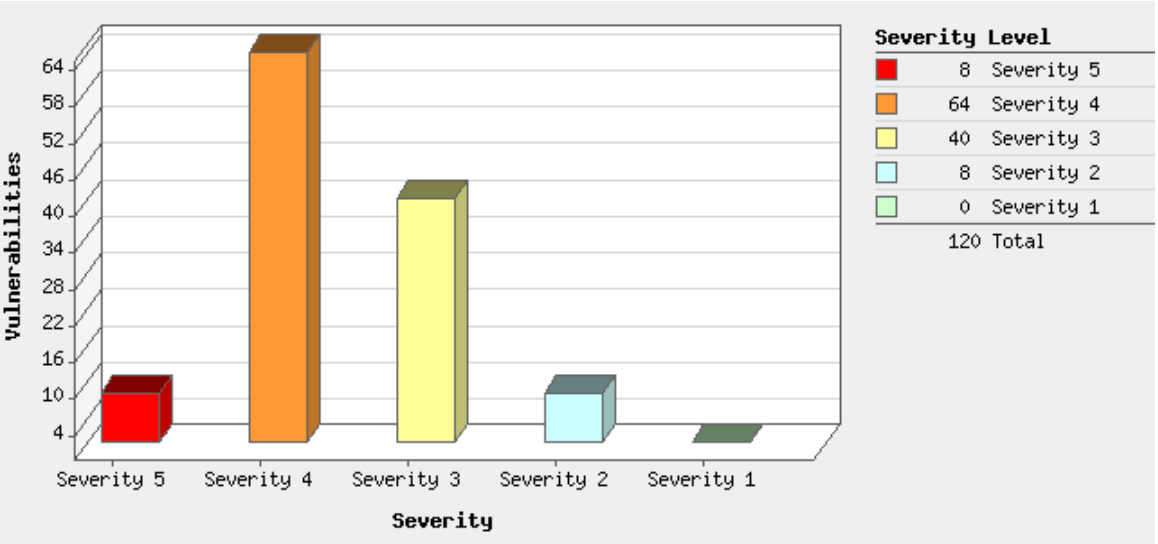
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	8	0	0	8
4	64	1	0	65
3	40	2	12	54
2	8	2	52	62
1	0	0	111	111
Total	120	5	175	300

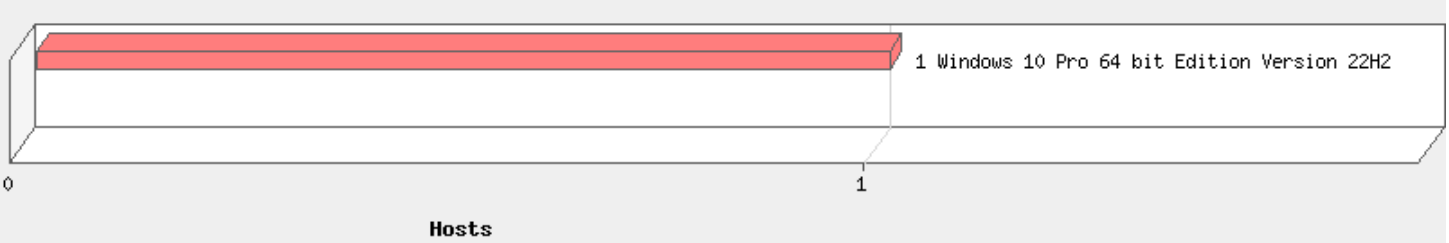
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Local	72	1	4	77
Windows	45	1	23	69
Security Policy	2	2	62	66
Information gathering	0	1	64	65
TCP/IP	0	0	7	7
Total	119	5	160	284

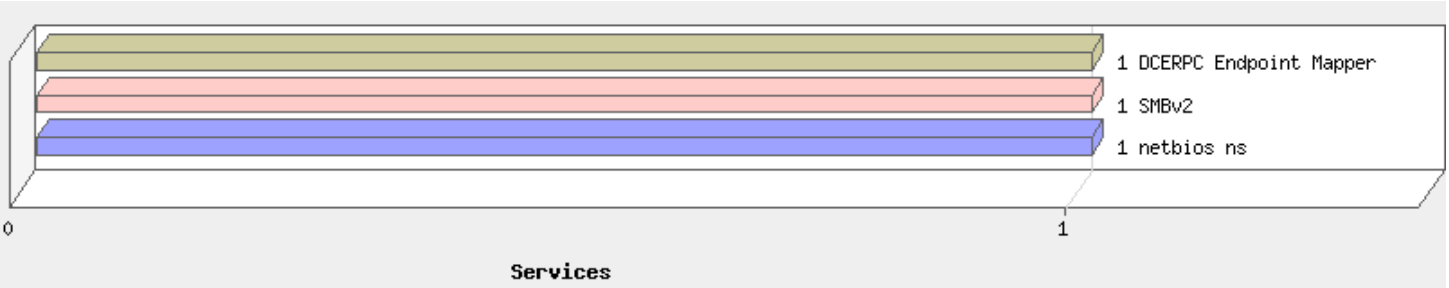
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

10.0.0.197 (desktop-ln5he01, DESKTOP-LN5HE01) Windows 10 Pro 64 bit Edition Version 22H2

Vulnerabilities (120)

5 Microsoft Windows Security Update for January 2024

QID:	92099
Category:	Windows
Associated CVEs:	CVE-2024-20666, CVE-2024-20674, CVE-2024-20654, CVE-2024-20657, CVE-2024-20658, CVE-2024-20680, CVE-2024-20682, CVE-2024-20683, CVE-2024-20691, CVE-2024-20694, CVE-2022-35737, CVE-2024-20696, CVE-2024-20697, CVE-2024-20698, CVE-2024-20699, CVE-2024-20700, CVE-2024-21305, CVE-2024-21307, CVE-2024-21313, CVE-2024-20653, CVE-2024-20660, CVE-2024-20661, CVE-2024-20663, CVE-2024-20664, CVE-2024-21316, CVE-2024-20681, CVE-2024-20687, CVE-2024-20692, CVE-2024-21306, CVE-2024-21309,

Vendor Reference:	CVE-2024-21310, CVE-2024-21311, CVE-2024-21314, CVE-2024-21320, CVE-2024-20652 KB5034119, KB5034121, KB5034122, KB5034123, KB5034127, KB5034129, KB5034130, KB5034134, KB5034167, KB5034169, KB5034171, KB5034173, KB5034176, KB5034184
Bugtraq ID:	-
Service Modified:	05/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - January 2024

Patch version is 10.0.20348.2227 for KB5034129 (https://support.microsoft.com/en-in/help/5034129)
Patch version is 10.0.17763.5329 for KB5034127 (https://support.microsoft.com/en-in/help/5034127)
Patch version is 10.0.14393.6614 for KB5034119 (https://support.microsoft.com/en-in/help/5034119)
Patch version is 10.0.10240.20402 for KB5034134 (https://support.microsoft.com/en-in/help/5034134)
Patch version is 10.0.22631.3007 for KB5034123 (https://support.microsoft.com/en-in/help/5034123)
Patch version is 10.0.19045.3930 for KB5034122 (https://support.microsoft.com/en-in/help/5034122)
Patch version is 10.0.22000.2713 for KB5034121 (https://support.microsoft.com/en-in/help/5034121)
Patch version is 10.0.25398.643 for KB5034130 (https://support.microsoft.com/en-in/help/5034130)
Patch version is 6.3.9600.21765 for KB5034171 (https://support.microsoft.com/en-in/help/5034171)
Patch version is 6.2.9200.24664 for KB5034184 (https://support.microsoft.com/en-in/help/5034184)
Patch version is 6.1.7601.26910 for KB5034169 (https://support.microsoft.com/en-in/help/5034169)
Patch version is 6.1.7601.26910 for KB5034167 (https://support.microsoft.com/en-in/help/5034167)
Patch version is 6.0.6003.22464 for KB5034173 (https://support.microsoft.com/en-in/help/5034173)
Patch version is 6.0.6003.22464 for KB5034176 (https://support.microsoft.com/en-in/help/5034176)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5034129 (https://support.microsoft.com/en-in/help/5034129)
KB5034127 (https://support.microsoft.com/en-in/help/5034127)
KB5034119 (https://support.microsoft.com/en-in/help/5034119)
KB5034134 (https://support.microsoft.com/en-in/help/5034134)
KB5034123 (https://support.microsoft.com/en-in/help/5034123)
KB5034122 (https://support.microsoft.com/en-in/help/5034122)
KB5034121 (https://support.microsoft.com/en-in/help/5034121)
KB5034130 (https://support.microsoft.com/en-in/help/5034130)
KB5034171 (https://support.microsoft.com/en-in/help/5034171)
KB5034184 (https://support.microsoft.com/en-in/help/5034184)
KB5034169 (https://support.microsoft.com/en-in/help/5034169)
KB5034167 (https://support.microsoft.com/en-in/help/5034167)
KB5034173 (https://support.microsoft.com/en-in/help/5034173)
KB5034176 (https://support.microsoft.com/en-in/help/5034176)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5034127 (https://support.microsoft.com/en-in/help/5034127)

KB5034129 (https://support.microsoft.com/en-in/help/5034129)

KB5034130 (https://support.microsoft.com/en-in/help/5034130)

KB5034121 (https://support.microsoft.com/en-in/help/5034121)

KB5034122 (https://support.microsoft.com/en-in/help/5034122)

KB5034123 (https://support.microsoft.com/en-in/help/5034123)

KB5034119 (https://support.microsoft.com/en-in/help/5034119)

KB5034134 (https://support.microsoft.com/en-in/help/5034134)

KB5034167 (https://support.microsoft.com/en-in/help/5034167)

KB5034169 (https://support.microsoft.com/en-in/help/5034169)

KB5034171 (https://support.microsoft.com/en-in/help/5034171)

KB5034173 (https://support.microsoft.com/en-in/help/5034173)

KB5034176 (https://support.microsoft.com/en-in/help/5034176)

KB5034184 (https://support.microsoft.com/en-in/help/5034184)

KB5034184 (https://support.microsoft.com/en-us/topic/january-9-2024-kb5034184-monthly-rollup-bc4d457f-c439-439d-9c32-400e5845d089)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-35737
Description: SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.
Link: https://blog.trailofbits.com/2022/10/25/sqlite-vulnerability-july-2022-library-api/

github-exploits

Reference: CVE-2022-35737
Description: trailofbits/publications exploit repository
Link: https://github.com/trailofbits/publications

Reference: CVE-2024-20698
Description: RomanRybachek/CVE-2024-20698 exploit repository
Link: https://github.com/RomanRybachek/CVE-2024-20698

Reference: CVE-2024-21305
Description: tandasat/CVE-2024-21305 exploit repository
Link: https://github.com/tandasat/CVE-2024-21305

Reference: CVE-2024-21306
Description: d4rks1d33/C-PoC-for-CVE-2024-21306 exploit repository
Link: https://github.com/d4rks1d33/C-PoC-for-CVE-2024-21306

Reference: CVE-2024-21306
Description: PhucHauDeveloper/BadbBlue exploit repository
Link: https://github.com/PhucHauDeveloper/BadbBlue

Reference: CVE-2024-21306
Description: PhucHauDeveloper/BadBlue exploit repository
Link: https://github.com/PhucHauDeveloper/BadBlue

gitee-exploits

Reference: CVE-2024-21305
Description: river3587/CVE-2024-21305 exploit repository
Link: https://gitee.com/river3587/CVE-2024-21305

nist-nvd2

Reference: CVE-2022-35737
Description: SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.
Link: https://blog.trailofbits.com/2022/10/25/sqlite-vulnerability-july-2022-library-api/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5034122 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 Microsoft Windows Security Update for February 2024

QID:	92111
Category:	Windows
Associated CVEs:	CVE-2024-21342, CVE-2024-21377, CVE-2024-21420, CVE-2024-21412, CVE-2024-21406, CVE-2024-21405, CVE-2024-21391, CVE-2024-21375, CVE-2024-21372, CVE-2024-21371, CVE-2024-21370, CVE-2024-21369, CVE-2024-21368, CVE-2024-21367, CVE-2024-21366, CVE-2024-21365, CVE-2024-21363, CVE-2024-21362, CVE-2024-21361, CVE-2024-21360, CVE-2024-21359, CVE-2024-21358, CVE-2024-21357, CVE-2024-21356, CVE-2024-21355, CVE-2024-21354, CVE-2024-21352, CVE-2024-21351, CVE-2024-21350, CVE-2024-21349, CVE-2024-21348, CVE-2024-21347, CVE-2024-21346, CVE-2024-21344, CVE-2024-21343, CVE-2024-21341, CVE-2024-21340, CVE-2024-21339, CVE-2024-21338, CVE-2024-21304, CVE-2024-20684, CVE-2024-21315
Vendor Reference:	KB5034795, KB5034833, KB5034767, KB5034774, KB5034769, KB5034765, KB5034763, KB5034766, KB5034770, KB5034768, KB5034819, KB5034830, KB5034831, KB5034809
Bugtraq ID:	-
Service Modified:	08/02/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - February 2024

Patch version is 6.0.6003.22510 for KB5034795 (https://support.microsoft.com/en-in/help/5034795)
Patch version is 6.0.6003.22510 for KB5034833 (https://support.microsoft.com/en-in/help/5034833)
Patch version is 10.0.14393.6707 for KB5034767 (https://support.microsoft.com/en-in/help/5034767)
Patch version is 10.0.10240.20466 for KB5034774 (https://support.microsoft.com/en-in/help/5034774)
Patch version is 10.0.25398.709 for KB5034769 (https://support.microsoft.com/en-in/help/5034769)
Patch version is 10.0.22621.3155 for KB5034765 (https://support.microsoft.com/en-in/help/5034765)
Patch version is 10.0.19041.4046 for KB5034763 (https://support.microsoft.com/en-in/help/5034763)
Patch version is 10.0.22000.2777 for KB5034766 (https://support.microsoft.com/en-in/help/5034766)
Patch version is 10.0.20348.2322 for KB5034770 (https://support.microsoft.com/en-in/help/5034770)
Patch version is 10.0.17763.5458 for KB5034768 (https://support.microsoft.com/en-in/help/5034768)
Patch version is 6.3.9600.21811 for KB5034819 (https://support.microsoft.com/en-in/help/5034819)
Patch version is 6.2.9200.24709 for KB5034830 (https://support.microsoft.com/en-in/help/5034830)
Patch version is 6.1.7601.26958 for KB5034831 (https://support.microsoft.com/en-in/help/5034831)
Patch version is 6.1.7601.26958 for KB5034809 (https://support.microsoft.com/en-in/help/5034809)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5034795 (https://support.microsoft.com/en-in/help/5034795)
KB5034833 (https://support.microsoft.com/en-in/help/5034833)
KB5034767 (https://support.microsoft.com/en-in/help/5034767)
KB5034774 (https://support.microsoft.com/en-in/help/5034774)
KB5034769 (https://support.microsoft.com/en-in/help/5034769)
KB5034765 (https://support.microsoft.com/en-in/help/5034765)
KB5034763 (https://support.microsoft.com/en-in/help/5034763)
KB5034766 (https://support.microsoft.com/en-in/help/5034766)
KB5034770 (https://support.microsoft.com/en-in/help/5034770)
KB5034768 (https://support.microsoft.com/en-in/help/5034768)
KB5034819 (https://support.microsoft.com/en-in/help/5034819)
KB5034830 (https://support.microsoft.com/en-in/help/5034830)
KB5034831 (https://support.microsoft.com/en-in/help/5034831)
KB5034809 (https://support.microsoft.com/en-in/help/5034809)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5034795 (https://support.microsoft.com/en-in/help/5034795)

KB5034833 (https://support.microsoft.com/en-in/help/5034833)

KB5034767 (https://support.microsoft.com/en-in/help/5034767)

KB5034774 (https://support.microsoft.com/en-in/help/5034774)

KB5034769 (https://support.microsoft.com/en-in/help/5034769)

KB5034765 (https://support.microsoft.com/en-in/help/5034765)

KB5034763 (https://support.microsoft.com/en-in/help/5034763)

KB5034766 (https://support.microsoft.com/en-in/help/5034766)

KB5034770 (https://support.microsoft.com/en-in/help/5034770)

KB5034768 (https://support.microsoft.com/en-in/help/5034768)

KB5034819 (https://support.microsoft.com/en-in/help/5034819)

KB5034830 (https://support.microsoft.com/en-in/help/5034830)

KB5034831 (https://support.microsoft.com/en-in/help/5034831)

KB5034809 (https://support.microsoft.com/en-in/help/5034809)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb

Reference: CVE-2024-21338
Description: Microsoft Windows 10.0.17763.5458 - Kernel Privilege Escalation
Link: https://www.exploit-db.com/exploits/51946

packetstorm

Reference: CVE-2024-21338
Description: Microsoft Windows 10.0.17763.5458 Privilege Escalation
Link: https://packetstormsecurity.com/files/177869/Microsoft-Windows-10.0.17763.5458-Privilege-Escalation.html

0day.today

Reference: CVE-2024-21338
Description: Microsoft Windows 10.0.17763.5458 - Kernel Privilege Escalation Exploit
Link: https://0day.today/exploit/39515

github-exploits

Reference: CVE-2024-21338
Description: UMU618/CVE-2024-21338 exploit repository
Link: https://github.com/UMU618/CVE-2024-21338

Reference: CVE-2024-21338
Description: hakaioffsec/CVE-2024-21338 exploit repository
Link: https://github.com/hakaioffsec/CVE-2024-21338

Reference: CVE-2024-21338
Description: varwara/CVE-2024-21338 exploit repository
Link: https://github.com/varwara/CVE-2024-21338

Reference: CVE-2024-21338
Description: tykawaii98/CVE-2024-21338_PoC exploit repository
Link: https://github.com/tykawaii98/CVE-2024-21338_PoC

Reference: CVE-2024-21338
Description: Crowdfense/CVE-2024-21338 exploit repository
Link: https://github.com/Crowdfense/CVE-2024-21338

coreimpact

Reference: CVE-2024-21412
Description: Microsoft Windows Internet Shortcut SmartScreen Bypass Exploit
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev

Reference: CVE-2024-21351
Description: Microsoft Windows SmartScreen Security Feature Bypass Vulnerability

Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-21412
Description: Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-21338
Description: Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2024-21338
Description: Windows Kernel Out-of-bounds in appid.sys AppLocker driver
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs
Reference: CVE-2024-21338
Description: Windows AppLocker Driver LPE Vulnerability - CVE-2024-21338
Link: https://www.crowdfense.com/windows-applocker-driver-lpe-vulnerability-cve-2024-21338/

nist-nvd2
Reference: CVE-2024-21338
Description: Windows Kernel Elevation of Privilege Vulnerability
Link: https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/

microsoft-cvrf
Reference: CVE-2024-21338
Description: Windows Kernel Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Feb?api-version=2020

Reference: CVE-2024-21351
Description: Windows SmartScreen Security Feature Bypass Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Feb?api-version=2020

Reference: CVE-2024-21412
Description: Internet Shortcut Files Security Feature Bypass Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Feb?api-version=2020

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2024-21412
Type: Exploit
Platform: Win32,Shortcut,Text,Binary,Document,Script

Malware ID: DarkGate
Type: Trojan
Platform: Shortcut

Malware ID: Generic
Type: Trojan
Platform: Win32

RESULTS:

KB5034763 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 Microsoft Windows Security Update for April 2024

QID:	92128
Category:	Windows
Associated CVEs:	CVE-2024-26180, CVE-2024-20678, CVE-2024-20669, CVE-2024-29064, CVE-2024-29062, CVE-2024-20665, CVE-2024-23594, CVE-2024-23593, CVE-2024-29050, CVE-2024-26229, CVE-2024-28901, CVE-2024-28923, CVE-2024-26240, CVE-2024-26216, CVE-2024-26241, CVE-2024-26218, CVE-2024-26194, CVE-2024-26217, CVE-2024-26214, CVE-2024-26172, CVE-2024-26254, CVE-2024-29052, CVE-2024-26253, CVE-2024-26252, CVE-2024-26230, CVE-2024-26212, CVE-2024-26244, CVE-2024-26213, CVE-2024-29061, CVE-2024-28907, CVE-2024-26226, CVE-2024-26220, CVE-2024-28903, CVE-2024-29066, CVE-2024-29056, CVE-2024-26239, CVE-2024-26211, CVE-2024-26232, CVE-2024-26243, CVE-2024-21447, CVE-2024-26245, CVE-2024-29988, CVE-2024-28898, CVE-2024-26236, CVE-2024-28904, CVE-2024-28902, CVE-2024-20688, CVE-2024-28905, CVE-2024-28900, CVE-2024-28897, CVE-2024-28896, CVE-2024-28925, CVE-2024-28924, CVE-2024-28919, CVE-2024-28921, CVE-2024-28922, CVE-2024-28920, CVE-2024-26228, CVE-2024-26215, CVE-2024-26208, CVE-2024-26207, CVE-2024-26242, CVE-2024-26237, CVE-2024-26235, CVE-2024-26234, CVE-2024-26210, CVE-2024-26158, CVE-2024-26205, CVE-2024-26200, CVE-2024-26179, CVE-2024-26256, CVE-2024-26255, CVE-2024-26250, CVE-2024-26248, CVE-2024-26219, CVE-2024-26209, CVE-2024-26202, CVE-2024-26195, CVE-2024-26189, CVE-2024-26183, CVE-2024-26175, CVE-2024-26171, CVE-2024-26168, CVE-2024-20693, CVE-2024-20689
Vendor Reference:	KB5036892, KB5036896, KB5036899, KB5036925, KB5036910, KB5036893, KB5036894, KB5036967, KB5036922, KB5036932, KB5036950, KB5036969, KB5036960, KB5036909
Bugtraq ID:	-
Service Modified:	08/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - April 2024

Patch version is 10.0.19041.4291 for KB5036892 (https://support.microsoft.com/en-in/help/5036892)
Patch version is 10.0.17763.5696 for KB5036896 (https://support.microsoft.com/en-in/help/5036896)
Patch version is 10.0.14393.6897 for KB5036899 (https://support.microsoft.com/en-in/help/5036899)
Patch version is 10.0.10240.20593 for KB5036925 (https://support.microsoft.com/en-in/help/5036925)
Patch version is 10.0.25398.830 for KB5036910 (https://support.microsoft.com/en-in/help/5036910)
Patch version is 10.0.22621.3447 for KB5036893 (https://support.microsoft.com/en-in/help/5036893)
Patch version is 10.0.22000.2899 for KB5036894 (https://support.microsoft.com/en-in/help/5036894)
Patch version is 6.1.7601.27066 for KB5036967 (https://support.microsoft.com/en-in/help/5036967)
Patch version is 6.1.7601.27066 for KB5036922 (https://support.microsoft.com/en-in/help/5036922)
Patch version is 6.0.6003.22616 for KB5036932 (https://support.microsoft.com/en-in/help/5036932)
Patch version is 6.0.6003.22616 for KB5036950 (https://support.microsoft.com/en-in/help/5036950)
Patch version is 6.2.9200.24819 for KB5036969 (https://support.microsoft.com/en-in/help/5036969)
Patch version is 6.3.9600.21919 for KB5036960 (https://support.microsoft.com/en-in/help/5036960)
Patch version is 10.0.20348.2400 for KB5036909 (https://support.microsoft.com/en-in/help/5036909)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5036892 (https://support.microsoft.com/en-in/help/5036892)
KB5036896 (https://support.microsoft.com/en-in/help/5036896)
KB5036899 (https://support.microsoft.com/en-in/help/5036899)
KB5036925 (https://support.microsoft.com/en-in/help/5036925)
KB5036910 (https://support.microsoft.com/en-in/help/5036910)
KB5036893 (https://support.microsoft.com/en-in/help/5036893)
KB5036894 (https://support.microsoft.com/en-in/help/5036894)
KB5036967 (https://support.microsoft.com/en-in/help/5036967)
KB5036922 (https://support.microsoft.com/en-in/help/5036922)
KB5036932 (https://support.microsoft.com/en-in/help/5036932)
KB5036950 (https://support.microsoft.com/en-in/help/5036950)
KB5036969 (https://support.microsoft.com/en-in/help/5036969)

KB5036960 (https://support.microsoft.com/en-in/help/5036960)
KB5036909 (https://support.microsoft.com/en-in/help/5036909)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5036892 (https://support.microsoft.com/en-in/help/5036892)

KB5036896 (https://support.microsoft.com/en-in/help/5036896)

KB5036899 (https://support.microsoft.com/en-in/help/5036899)

KB5036925 (https://support.microsoft.com/en-in/help/5036925)

KB5036910 (https://support.microsoft.com/en-in/help/5036910)

KB5036893 (https://support.microsoft.com/en-in/help/5036893)

KB5036894 (https://support.microsoft.com/en-in/help/5036894)

KB5036967 (https://support.microsoft.com/en-in/help/5036967)

KB5036922 (https://support.microsoft.com/en-in/help/5036922)

KB5036932 (https://support.microsoft.com/en-in/help/5036932)

KB5036950 (https://support.microsoft.com/en-in/help/5036950)

KB5036969 (https://support.microsoft.com/en-in/help/5036969)

KB5036960 (https://support.microsoft.com/en-in/help/5036960)

KB5036909 (https://support.microsoft.com/en-in/help/5036909)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2024-26218
Description: Windows PspBuildCreateProcessContext Double-Fetch / Buffer Overflow
Link: https://packetstormsecurity.com/files/178377/Windows-PspBuildCreateProcessContext-Double-Fetch-Buffer-Overflow.html

Reference: CVE-2024-26218
Description: undefinedExploiting The NT Kernel In 24H2undefined
Link: https://packetstormsecurity.com/files/178378/undefinedExploiting-The-NT-Kernel-In-24H2undefined.html

Reference: CVE-2024-26229
Description: Firebeam CVE-2024-26229 Plugin
Link: https://packetstormsecurity.com/files/179962/Firebeam-CVE-2024-26229-Plugin.html

Reference: CVE-2024-26218
Description: Exploiting The NT Kernel In 24H2
Link: https://packetstormsecurity.com/files/178378/Exploiting-The-NT-Kernel-In-24H2.html

github-exploits

Reference: CVE-2024-26218
Description: exploits-forsale/CVE-2024-26218 exploit repository
Link: https://github.com/exploits-forsale/CVE-2024-26218

Reference: CVE-2024-26229
Description: 0XJ175/DRive exploit repository
Link: https://github.com/0XJ175/DRive

Reference: CVE-2024-26229
Description: NVISOsecurity/CVE-2024-26229-BOF exploit repository
Link: https://github.com/NVISOsecurity/CVE-2024-26229-BOF

Reference: CVE-2024-26229
Description: apkc/CVE-2024-26229-BOF exploit repository
Link: https://github.com/apkc/CVE-2024-26229-BOF

Reference: CVE-2024-26229
Description: Cracked5pider/eop24-26229 exploit repository
Link: https://github.com/Cracked5pider/eop24-26229

Reference: CVE-2024-26230
Description: kiwids0220/CVE-2024-26230 exploit repository
Link: https://github.com/kiwids0220/CVE-2024-26230

Reference: CVE-2024-26229
Description: RalfHacker/CVE-2024-26229-exploit exploit repository
Link: https://github.com/RalfHacker/CVE-2024-26229-exploit

Reference: CVE-2024-26229
Description: varwara/CVE-2024-26229 exploit repository
Link: https://github.com/varwara/CVE-2024-26229

Reference: CVE-2024-26230
Description: Wa1nut4/CVE-2024-26230 exploit repository
Link: https://github.com/Wa1nut4/CVE-2024-26230

cisa-kev
Reference: CVE-2024-29988
Description: Microsoft SmartScreen Prompt Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

blogs
Reference: CVE-2024-26230
Description: A trick, the story of CVE-2024-26230
Link: https://whereisk0shl.top/post/a-trick-the-story-of-cve-2024-26230

microsoft-cvrf
Reference: CVE-2024-26234
Description: Proxy Driver Spoofing Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Apr?api-version=2020

ASSOCIATED MALWARE:
ReversingLabs
Malware ID: CVE-2024-26234
Type: Exploit
Platform: Win32

Malware ID: CVE-2024-26229
Type: Exploit
Platform: Win32,Win64

RESULTS:

KB5036892 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 Microsoft Windows Security Update for July 2024

QID: 92149
Category: Windows
Associated CVEs: CVE-2024-39684, CVE-2024-38517, CVE-2024-38112, CVE-2024-38105, CVE-2024-38104, CVE-2024-38102, CVE-2024-38101, CVE-2024-38100, CVE-2024-38099, CVE-2024-38091, CVE-2024-38085, CVE-2024-38080, CVE-2024-38079, CVE-2024-38078, CVE-2024-38077, CVE-2024-38076, CVE-2024-38074, CVE-2024-38073, CVE-2024-38072, CVE-2024-38071, CVE-2024-38070, CVE-2024-38069, CVE-2024-38068, CVE-2024-38067, CVE-2024-38066, CVE-2024-38065, CVE-2024-38064, CVE-2024-38062, CVE-2024-38061, CVE-2024-38060, CVE-2024-38059, CVE-2024-38058, CVE-2024-38057, CVE-2024-38056, CVE-2024-38055, CVE-2024-38054, CVE-2024-38053, CVE-2024-38052, CVE-2024-38051, CVE-2024-38050,

	CVE-2024-38049, CVE-2024-38048, CVE-2024-38047, CVE-2024-38044, CVE-2024-38043, CVE-2024-38041, CVE-2024-38034, CVE-2024-38033, CVE-2024-38032, CVE-2024-38031, CVE-2024-38030, CVE-2024-38028, CVE-2024-38027, CVE-2024-38025, CVE-2024-38022, CVE-2024-38019, CVE-2024-38017, CVE-2024-38015, CVE-2024-38013, CVE-2024-38011, CVE-2024-38010, CVE-2024-37989, CVE-2024-37988, CVE-2024-37987, CVE-2024-37986, CVE-2024-37985, CVE-2024-37984, CVE-2024-37981, CVE-2024-37978, CVE-2024-37977, CVE-2024-37975, CVE-2024-37974, CVE-2024-37973, CVE-2024-37972, CVE-2024-37971, CVE-2024-37970, CVE-2024-37969, CVE-2024-3596, CVE-2024-35270, CVE-2024-30098, CVE-2024-30081, CVE-2024-30079, CVE-2024-30071, CVE-2024-30013, CVE-2024-28899, CVE-2024-26184, CVE-2024-21417, CVE-2024-38186, CVE-2024-38187, CVE-2024-38185, CVE-2024-38165, CVE-2024-38191, CVE-2024-38184, CVE-2024-38161
Vendor Reference:	KB5040430, KB5040434, KB5040448, KB5040438, KB5040442, KB5040427, KB5040431, KB5040437, KB5040456, KB5040485, KB5040497, KB5040498, KB5040499, KB5040490
Bugtraq ID:	-
Service Modified:	09/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - July 2024

Patch version is 10.0.17763.6054 for KB5040430 (https://support.microsoft.com/en-in/help/5040430)
Patch version is 10.0.14393.7155 for KB5040434 (https://support.microsoft.com/en-in/help/5040434)
Patch version is 10.0.10240.20708 for KB5040448 (https://support.microsoft.com/en-in/help/5040448)
Patch version is 10.0.25398.1009 for KB5040438 (https://support.microsoft.com/en-in/help/5040438)
Patch version is 10.0.22621.3880 for KB5040442 (https://support.microsoft.com/en-in/help/5040442)
Patch version is 10.0.19041.4648 for KB5040427 (https://support.microsoft.com/en-in/help/5040427)
Patch version is 10.0.22000.3079 for KB5040431 (https://support.microsoft.com/en-in/help/5040431)
Patch version is 10.0.20348.2582 for KB5040437 (https://support.microsoft.com/en-in/help/5040437)
Patch version is 6.3.9600.22073 for KB5040456 (https://support.microsoft.com/en-in/help/5040456)
Patch version is 6.2.9200.24975 for KB5040485 (https://support.microsoft.com/en-in/help/5040485)
Patch version is 6.1.7601.27216 for KB5040497 (https://support.microsoft.com/en-in/help/5040497)
Patch version is 6.1.7601.27216 for KB5040498 (https://support.microsoft.com/en-in/help/5040498)
Patch version is 6.0.6003.22768 for KB5040499 (https://support.microsoft.com/en-in/help/5040499)
Patch version is 6.0.6003.22768 for KB5040490 (https://support.microsoft.com/en-in/help/5040490)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5040430 (https://support.microsoft.com/en-in/help/5040430)
KB5040434 (https://support.microsoft.com/en-in/help/5040434)
KB5040448 (https://support.microsoft.com/en-in/help/5040448)
KB5040438 (https://support.microsoft.com/en-in/help/5040438)
KB5040442 (https://support.microsoft.com/en-in/help/5040442)
KB5040427 (https://support.microsoft.com/en-in/help/5040427)
KB5040431 (https://support.microsoft.com/en-in/help/5040431)
KB5040437 (https://support.microsoft.com/en-in/help/5040437)
KB5040456 (https://support.microsoft.com/en-in/help/5040456)
KB5040485 (https://support.microsoft.com/en-in/help/5040485)
KB5040497 (https://support.microsoft.com/en-in/help/5040497)
KB5040498 (https://support.microsoft.com/en-in/help/5040498)
KB5040499 (https://support.microsoft.com/en-in/help/5040499)
KB5040490 (https://support.microsoft.com/en-in/help/5040490)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5040430 (https://support.microsoft.com/en-in/help/5040430)

KB5040434 (https://support.microsoft.com/en-in/help/5040434)

KB5040448 (https://support.microsoft.com/en-in/help/5040448)

KB5040438 (https://support.microsoft.com/en-in/help/5040438)

KB5040442 (https://support.microsoft.com/en-in/help/5040442)

KB5040427 (https://support.microsoft.com/en-in/help/5040427)

KB5040431 (https://support.microsoft.com/en-in/help/5040431)

KB5040437 (https://support.microsoft.com/en-in/help/5040437)

KB5040456 (https://support.microsoft.com/en-in/help/5040456)

KB5040485 (https://support.microsoft.com/en-in/help/5040485)

KB5040497 (https://support.microsoft.com/en-in/help/5040497)

KB5040498 (https://support.microsoft.com/en-in/help/5040498)

KB5040499 (https://support.microsoft.com/en-in/help/5040499)

KB5040490 (https://support.microsoft.com/en-in/help/5040490)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2024-3596
Description: alperenugurlu/CVE-2024-3596-Detector exploit repository
Link: https://github.com/alperenugurlu/CVE-2024-3596-Detector

Reference: CVE-2024-38077
Description: CloudCrowSec001/CVE-2024-38077-POC exploit repository
Link: https://github.com/CloudCrowSec001/CVE-2024-38077-POC

Reference: CVE-2024-38077
Description: qi4L/CVE-2024-38077 exploit repository
Link: https://github.com/qi4L/CVE-2024-38077

Reference: CVE-2024-38077
Description: Wlibang/CVE-2024-38077 exploit repository
Link: https://github.com/Wlibang/CVE-2024-38077

Reference: CVE-2024-38041
Description: varwara/CVE-2024-38041 exploit repository
Link: https://github.com/varwara/CVE-2024-38041

Reference: CVE-2024-38080
Description: pwndorei/CVE-2024-38080 exploit repository
Link: https://github.com/pwndorei/CVE-2024-38080

cisa-kev

Reference: CVE-2024-38112
Description: Microsoft Windows MSHTML Platform Spoofing Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-38080
Description: Microsoft Windows Hyper-V Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2024-38080
Description: Microsoft Windows Hyper-V Elevation of Privilege Vulnerability
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2024-38080
Description: [Research] Hyper-V 1-day Class: CVE-2024-38080
Link: https://hackyboiz.github.io/2024/09/01/pwndorei/hyperv-1dayclass_CVE-2024-38080/

Reference: CVE-2024-38061
Description: Three-Headed Potato Dog
Link: https://blog.compass-security.com/2024/09/three-headed-potato-dog/

microsoft-cvrf

Reference: CVE-2024-38112
Description: Windows MSHTML Platform Spoofing Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Jul?api-version=2020

Reference: CVE-2024-38080
Description: Windows Hyper-V Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Jul?api-version=2020

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2024-38112
Type: Exploit
Platform: Win32

RESULTS:

KB5040427 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 Microsoft Windows Security Update for August 2024

QID:	92160
Category:	Windows
Associated CVEs:	CVE-2024-38155, CVE-2024-38152, CVE-2024-38146, CVE-2024-38143, CVE-2024-38140, CVE-2024-38134, CVE-2024-38127, CVE-2024-38122, CVE-2024-38117, CVE-2024-38114, CVE-2024-38106, CVE-2024-38193, CVE-2024-38178, CVE-2024-38223, CVE-2024-38215, CVE-2024-38214, CVE-2024-38120, CVE-2022-3775, CVE-2024-38180, CVE-2024-38154, CVE-2024-38153, CVE-2024-38151, CVE-2024-38150, CVE-2024-38148, CVE-2024-38147, CVE-2024-38145, CVE-2024-38144, CVE-2024-38142, CVE-2024-38141, CVE-2024-38138, CVE-2024-38137, CVE-2024-38136, CVE-2024-38135, CVE-2024-38133, CVE-2024-38132, CVE-2024-38131, CVE-2024-38130, CVE-2024-38128, CVE-2024-38126, CVE-2024-38125, CVE-2024-38121, CVE-2024-38118, CVE-2024-38116, CVE-2024-38115, CVE-2024-29995, CVE-2024-38107, CVE-2023-40547, CVE-2024-38198, CVE-2024-38196, CVE-2024-38123, CVE-2022-2601
Vendor Reference:	KB5041571, KB5041585, KB5041580, KB5041592, KB5041160, KB5041773, KB5041782, KB5041573, KB5041578, KB5041851, KB5041838, KB5041823, KB5041850, KB5041847, KB5041828
Bugtraq ID:	-
Service Modified:	09/17/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - August 2024

KB5041571 (https://support.microsoft.com/en-in/help/5041571)
KB5041585 (https://support.microsoft.com/en-in/help/5041585)
KB5041580 (https://support.microsoft.com/en-in/help/5041580)
KB5041592 (https://support.microsoft.com/en-in/help/5041592)
KB5041160 (https://support.microsoft.com/en-in/help/5041160)
KB5041773 (https://support.microsoft.com/en-in/help/5041773)
KB5041782 (https://support.microsoft.com/en-in/help/5041782)
KB5041573 (https://support.microsoft.com/en-in/help/5041573)
KB5041578 (https://support.microsoft.com/en-in/help/5041578)
KB5041851 (https://support.microsoft.com/en-in/help/5041851)
KB5041838 (https://support.microsoft.com/en-in/help/5041838)

KB5041823 (https://support.microsoft.com/en-in/help/5041823)
KB5041850 (https://support.microsoft.com/en-in/help/5041850)
KB5041847 (https://support.microsoft.com/en-in/help/5041847)
KB5041828 (https://support.microsoft.com/en-in/help/5041828)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5041571 (https://support.microsoft.com/en-in/help/5041571)
KB5041585 (https://support.microsoft.com/en-in/help/5041585)
KB5041580 (https://support.microsoft.com/en-in/help/5041580)
KB5041592 (https://support.microsoft.com/en-in/help/5041592)
KB5041160 (https://support.microsoft.com/en-in/help/5041160)
KB5041773 (https://support.microsoft.com/en-in/help/5041773)
KB5041782 (https://support.microsoft.com/en-in/help/5041782)
KB5041573 (https://support.microsoft.com/en-in/help/5041573)
KB5041578 (https://support.microsoft.com/en-in/help/5041578)
KB5041851 (https://support.microsoft.com/en-in/help/5041851)
KB5041838 (https://support.microsoft.com/en-in/help/5041838)
KB5041823 (https://support.microsoft.com/en-in/help/5041823)
KB5041850 (https://support.microsoft.com/en-in/help/5041850)
KB5041847 (https://support.microsoft.com/en-in/help/5041847)
KB5041828 (https://support.microsoft.com/en-in/help/5041828)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5041571 (https://support.microsoft.com/en-in/help/5041571)

KB5041585 (https://support.microsoft.com/en-in/help/5041585)

KB5041580 (https://support.microsoft.com/en-in/help/5041580)

KB5041592 (https://support.microsoft.com/en-in/help/5041592)

KB5041160 (https://support.microsoft.com/en-in/help/5041160)

KB5041773 (https://support.microsoft.com/en-in/help/5041773)

KB5041782 (https://support.microsoft.com/en-in/help/5041782)

KB5041573 (https://support.microsoft.com/en-in/help/5041573)

KB5041578 (https://support.microsoft.com/en-in/help/5041578)

KB5041851 (https://support.microsoft.com/en-in/help/5041851)

KB5041838 (https://support.microsoft.com/en-in/help/5041838)

KB5041823 (https://support.microsoft.com/en-in/help/5041823)

KB5041850 (https://support.microsoft.com/en-in/help/5041850)

KB5041847 (https://support.microsoft.com/en-in/help/5041847)

KB5041828 (https://support.microsoft.com/en-in/help/5041828)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits
- Reference: CVE-2024-38127
- Description: pwndorei/CVE-2024-38127 exploit repository
- Link: https://github.com/pwndorei/CVE-2024-38127

cisa-kev
- Reference: CVE-2024-38106
- Description: Microsoft Windows Kernel Privilege Escalation Vulnerability
- Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

- Reference: CVE-2024-38193
- Description: Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability
- Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-38178
Description: Microsoft Windows Scripting Engine Memory Corruption Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-38107
Description: Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2024-38106
Description: Microsoft Windows Windows Kernel Elevation of Privilege Vulnerability
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2024-38193
Description: Microsoft Windows Windows Ancillary Function Driver for WinSock Elevation of Privilege (use after free)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2024-38178
Description: Microsoft Windows Scripting Engine Memory Corruption Vulnerability
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2024-38107
Description: Microsoft Windows Windows Power Dependency Coordinator Elevation of Privilege (use after free)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2024-38106
Description: Dissecting the CVE-2024-38106 Fix
Link: https://www.pixiepointsecurity.com/blog/nday-cve-2024-38106/

microsoft-cvrf

Reference: CVE-2024-38106
Description: Windows Kernel Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Aug?api-version=2020

Reference: CVE-2024-38193
Description: Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Aug?api-version=2020

Reference: CVE-2024-38178
Description: Scripting Engine Memory Corruption Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Aug?api-version=2020

Reference: CVE-2024-38107
Description: Windows Power Dependency Coordinator Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Aug?api-version=2020

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5041580 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 Microsoft Windows Transmission Control Protocol/Internet Protocol (TCP/IP) Remote Code Execution (RCE) Vulnerability for August 2024

QID: 92165
Category: Windows
Associated CVEs: CVE-2024-38063

Vendor Reference:	CVE-2024-38063
Bugtraq ID:	-
Service Modified:	09/12/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote code execution vulnerability exists in Microsoft Windows TCP/IP.

Patch version is 10.0.26100.1455 for KB5041571 (https://support.microsoft.com/en-in/help/5041571)
Patch version is 10.0.22621.4036 for KB5041585 (https://support.microsoft.com/en-in/help/5041585)
Patch version is 10.0.19041.4780 for KB5041580 (https://support.microsoft.com/en-in/help/5041580)
Patch version is 10.0.22000.3147 for KB5041592 (https://support.microsoft.com/en-in/help/5041592)
Patch version is 10.0.20348.2652 for KB5041160 (https://support.microsoft.com/en-in/help/5041160)
Patch version is 10.0.14393.7254 for KB5041773 (https://support.microsoft.com/en-in/help/5041773)
Patch version is 10.0.10240.20747 for KB5041782 (https://support.microsoft.com/en-in/help/5041782)
Patch version is 10.0.25398.1085 for KB5041573 (https://support.microsoft.com/en-in/help/5041573)
Patch version is 10.0.17763.6189 for KB5041578 (https://support.microsoft.com/en-in/help/5041578)
Patch version is 6.2.9200.25016 for KB5041851 (https://support.microsoft.com/en-in/help/5041851)
Patch version is 6.1.7601.27265 for KB5041838 (https://support.microsoft.com/en-in/help/5041838)
Patch version is 6.1.7601.27265 for KB5041823 (https://support.microsoft.com/en-in/help/5041823)
Patch version is 6.0.6003.22814 for KB5041850 (https://support.microsoft.com/en-in/help/5041850)
Patch version is 6.0.6003.22814 for KB5041847 (https://support.microsoft.com/en-in/help/5041847)
Patch version is 6.3.9600.22131 for KB5041828 (https://support.microsoft.com/en-in/help/5041828)

IMPACT:

An unauthenticated attacker could repeatedly send IPv6 packets, that include specially crafted packets, to a Windows machine which could enable remote code execution.

SOLUTION:

Customers are advised to refer to CVE-2024-38063 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063) for more information pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-38063 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference:	CVE-2024-38063
Description:	Microsoft Windows IPv6 Memory Corruption
Link:	https://packetstormsecurity.com/files/180422/Microsoft-Windows-IPv6-Memory-Corruption.html
Reference:	CVE-2024-38063
Description:	Microsoft Windows IPv6 CVE-2024-38063 Checker / Denial Of Service
Link:	https://packetstormsecurity.com/files/180458/Microsoft-Windows-IPv6-CVE-2024-38063-Checker-Denial-Of-Service.html

0day.today

Reference:	CVE-2024-38063
Description:	Windows TCP/IP - Remote Code Execution Checker and Denial of Service Exploit
Link:	https://0day.today/exploit/39735

github-exploits

Reference:	CVE-2024-38063
Description:	PumpkinBridge/Windows-CVE-2024-38063 exploit repository
Link:	https://github.com/PumpkinBridge/Windows-CVE-2024-38063
Reference:	CVE-2024-38063

Description: ps-interactive/cve-2024-38063 exploit repository
Link: https://github.com/ps-interactive/cve-2024-38063

Reference: CVE-2024-38063
Description: ThemeHackers/CVE-2024-38063 exploit repository
Link: https://github.com/ThemeHackers/CVE-2024-38063

Reference: CVE-2024-38063
Description: KernelKraze/CVE-2024-38063_PoC exploit repository
Link: https://github.com/KernelKraze/CVE-2024-38063_PoC

Reference: CVE-2024-38063
Description: Sachinart/CVE-2024-38063-poc exploit repository
Link: https://github.com/Sachinart/CVE-2024-38063-poc

Reference: CVE-2024-38063
Description: zenzue/CVE-2024-38063-POC exploit repository
Link: https://github.com/zenzue/CVE-2024-38063-POC

Reference: CVE-2024-38063
Description: AdminPentester/CVE-2024-38063- exploit repository
Link: https://github.com/AdminPentester/CVE-2024-38063-

Reference: CVE-2024-38063
Description: ynwarcs/CVE-2024-38063 exploit repository
Link: https://github.com/ynwarcs/CVE-2024-38063

Reference: CVE-2024-38063
Description: Faizan-Khanx/CVE-2024-38063 exploit repository
Link: https://github.com/Faizan-Khanx/CVE-2024-38063

blogs

Reference: CVE-2024-38063
Description: PoC for CVE-2024-38063 (RCE in tcpip.sys)
Link: https://darkwebinformer.com/poc-for-cve-2024-38063-rce-in-tcpip-sys/

Reference: CVE-2024-38063
Description: Exploiting the Windows Kernel via Malicious IPv6 Packets (CVE-2024-38063)
Link: https://malwaretech.com/2024/08/exploiting-CVE-2024-38063.html

vulncheck-initial-access

Reference: CVE-2024-38063
Description: IPv6 Network Stack Overflow DoS
Link: https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2024-38063

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IPAddress ['10.0.0.197' 'fe80::641e:149e:4486:57a1']
KB5041580 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

5 VideoLAN VLC Media player Stack smashing in SMB/CIFS access (VideoLAN-SA-1006)

QID: 376211
Category: Local
Associated CVEs: -
Vendor Reference: VideoLAN-SA-1006
Bugtraq ID: -
Service Modified: 02/11/2022

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:
VLC media player 1.1.4 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has confirmed the vulnerability and released VLC media player version 1.1.5 to resolve this issue. Download the latest version of vlc from here (https://www.videolan.org/vlc/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1006 (https://www.videolan.org/security/sa1006.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-47)

QID:	377768
Category:	Local
Associated CVEs:	CVE-2022-45413, CVE-2022-45410, CVE-2022-45418, CVE-2022-45412, CVE-2022-45406, CVE-2022-45409, CVE-2022-45408, CVE-2022-45405, CVE-2022-45417, CVE-2022-40674, CVE-2022-45404, CVE-2022-45419, CVE-2022-45403, CVE-2022-45411, CVE-2022-45407, CVE-2022-45416, CVE-2022-45421, CVE-2022-45415, CVE-2022-45420
Vendor Reference:	MFSA2022-47
Bugtraq ID:	-
Service Modified:	12/31/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2022-45403: Service Workers might have learned size of cross-origin media files
CVE-2022-45404: Fullscreen notification bypass
CVE-2022-45405: Use-after-free in InputStream implementation
CVE-2022-45406: Use-after-free of a JavaScript Realm

CVE-2022-45407: Loading fonts on workers was not thread-safe
CVE-2022-45408: Fullscreen notification bypass via windowName
CVE-2022-45409: Use-after-free in Garbage Collection
CVE-2022-45410: ServiceWorker-intercepted requests bypassed SameSite cookie policy
CVE-2022-45411: Cross-Site Tracing was possible via non-standard override headers
CVE-2022-45412: Symlinks may resolve to partially uninitialized buffers
CVE-2022-45413: SameSite=Strict cookies could have been sent cross-site via intent URLs
CVE-2022-40674: Use-after-free vulnerability in expat
CVE-2022-45415: Downloaded file may have been saved with malicious extension
CVE-2022-45416: Keystroke Side-Channel Leakage
CVE-2022-45417: Service Workers in Private Browsing Mode may have been written to disk
CVE-2022-45418: Custom mouse cursor could have been drawn over browser UI
CVE-2022-45419: Deleting a security exception did not take effect immediately
CVE-2022-45420: Iframe contents could be rendered outside the iframe
CVE-2022-45421: Memory safety bugs fixed in Firefox 107 and Firefox ESR 102.5

Affected Products:
Prior to Firefox 107

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2022-47 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2022-47 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Microsoft Windows Codecs Library Remote Code Execution Vulnerabilities - November 2020

QID:	91698
Category:	Windows
Associated CVEs:	CVE-2020-17101, CVE-2020-17105, CVE-2020-17102, CVE-2020-17079, CVE-2020-17081, CVE-2020-17082, CVE-2020-17086, CVE-2020-17078, CVE-2020-17106, CVE-2020-17109, CVE-2020-17108, CVE-2020-17110, CVE-2020-17107
Vendor Reference:	CVE-2020-17101, CVE-2020-17079, CVE-2020-17081, CVE-2020-17082, CVE-2020-17086, CVE-2020-17078, CVE-2020-17110, CVE-2020-17109, CVE-2020-17108, CVE-2020-17107, CVE-2020-17106, CVE-2020-17105, CVE-2020-17102
Bugtraq ID:	-
Service Modified:	01/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Multiple security vulnerabilities exist in Microsoft Windows Codecs Library.

Affected Product:

WebpImageExtension prior to 1.0.32731.0
HEIFImageExtension prior to 1.0.32532.0
AV1VideoExtension prior to1.1.32442.0
RawImageExtension prior to1.0.32861.0
HEVCVideoExtension prior to 1.0.32762.0

IMPACT:

An attacker who successfully exploited the vulnerability could execute arbitrary code.

SOLUTION:

Users are advised to check CVE-2020-17101 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17101),CVE-2020-17105 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17105),CVE-2020-17102 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17102),CVE-2020-17079 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17079),CVE-2020-17081 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17081),CVE-2020-17082 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17082),CVE-2020-17086 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17086),CVE-2020-17078 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17078),CVE-2020-17106 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17106),CVE-2020-17109 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17109),CVE-2020-17108 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17108),CVE-2020-17110 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17110),CVE-2020-17107 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17107) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Security Update Guide (https://msrc.microsoft.com/update-guide/en-us)

Microsoft Security Update Guide (https://support.microsoft.com/en-us/account-billing/get-updates-for-apps-and-games-in-microsoft-store-a1fe19c0-532d-ec47-7035-d1c5a1dd464f)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2020-17086
Description:	T81oub/CVE-2020-17086 exploit repository
Link:	https://github.com/T81oub/CVE-2020-17086

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.WebpImageExtension detected
Version '1.0.22753.0'
Microsoft vulnerable Microsoft.HEIFImageExtension detected
Version '1.0.22742.0'

4 Microsoft Windows Codecs Library and VP9 Video Extensions Multiple Vulnerabilities

QID:	91761
Category:	Windows
Associated CVEs:	CVE-2021-28466, CVE-2021-28464, CVE-2021-28468
Vendor Reference:	CVE-2021-28466, CVE-2021-28464, CVE-2021-28468
Bugtraq ID:	-
Service Modified:	04/15/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory.
Microsoft has disclosed Information Disclosure and Remote Code Execution in Windows Codecs Library and VP9 Video Extensions.

Affected Product:
VP9 Video Extensions prior to version 1.0.40631.0
Raw Image Extension prior to version 1.0.40392.0

IMPACT:

An attacker who successfully exploited this vulnerability could obtain information to further compromise the user system.

SOLUTION:

Users are advised to check CVE-2021-26902 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-26902) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-28317: Windows (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28317)

CVE-2021-28466: Windows (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28466)

CVE-2021-27079: Windows (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-27079)

CVE-2021-28464: Windows (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28464)

CVE-2021-28468: Windows (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28468)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'

 4 Microsoft Windows Codecs Library Web Media Extension Remote Code Execution Vulnerability

QID:	91764
Category:	Windows
Associated CVEs:	CVE-2021-28465
Vendor Reference:	CVE-2021-28465
Bugtraq ID:	-
Service Modified:	05/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory.

Affected Product:

Microsoft.WebMediaExtensions prior to version 1.0.40831.0

IMPACT:

An attacker who successfully exploited this vulnerability could lead to remote code execution.

SOLUTION:

Users are advised to check CVE-2021-28465 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28465) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.WebMediaExtensions detected
Version '1.0.20875.0'

4 Microsoft 3D Viewer Multiple Vulnerabilities - June 2021

QID:	91773
Category:	Windows
Associated CVEs:	CVE-2021-31944, CVE-2021-31943, CVE-2021-31942
Vendor Reference:	CVE-2021-31944, CVE-2021-31943, CVE-2021-31942
Bugtraq ID:	-
Service Modified:	07/02/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft 3D Viewer is prone to Remote Code Execution and Information Disclosure Vulnerability.

IMPACT:

Successful exploitation allows attacker to compromise the system.

SOLUTION:

Users are advised to check CVE-2021-31944 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31944), CVE-2021-31943 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31943) and CVE-2021-31942 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31942) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-31944 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31944)

CVE-2021-31943 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31943)

CVE-2021-31942 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31942)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.Microsoft3DViewer detected
Version '6.1908.2042.0'

4 Microsoft Paint 3D Remote Code Execution Vulnerability - June 2021

QID:	91774
Category:	Windows
Associated CVEs:	CVE-2021-31983, CVE-2021-31946, CVE-2021-31945
Vendor Reference:	CVE-2021-31983, CVE-2021-31946, CVE-2021-31945
Bugtraq ID:	-
Service Modified:	08/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Paint 3D is prone to Remote Code Execution Vulnerability.

IMPACT:

Successful exploitation allows attacker to compromise the system.

SOLUTION:

Users are advised to check CVE-2021-31983 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31983), CVE-2021-31946 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31946) and CVE-2021-31945 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31945) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-31983 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31983)

CVE-2021-31946 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31946)

CVE-2021-31945 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31945)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.MSPaint detected
Version '6.1907.29027.0'

4 Microsoft 3D Viewer Remote Code Execution (RCE) Vulnerability - November 2021

QID:	91834
Category:	Windows

Associated CVEs:	CVE-2021-43208, CVE-2021-43209
Vendor Reference:	CVE-2021-43208, CVE-2021-43209
Bugtraq ID:	-
Service Modified:	11/18/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft 3D Viewer is prone to Remote Code Execution Vulnerability.

Affected Versions:Microsoft 3D-Viewer App package versions prior to 7.2107.7012.0

IMPACT:

Successful exploitation allows an attacker to execute code remotely.

SOLUTION:

Users are advised to check CVE-2021-43208 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43208) and CVE-2021-43209 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43209) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

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

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.Microsoft3DViewer detected
Version '6.1908.2042.0'

4 Windows AppX Installer Spoofing Vulnerability

QID:	91848
Category:	Windows
Associated CVEs:	CVE-2021-43890
Vendor Reference:	CVE-2021-43890
Bugtraq ID:	-
Service Modified:	07/25/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

CVE-2021-43890: Windows AppX Installer Spoofing Vulnerability

Affected Products:

Windows 10 version Windows 10 version 1809 and later or any version of Windows 11
Windows 10 version 1709 or Windows 10 version 1803.

IMPACT:

An attacker could craft a malicious attachment to be used in phishing campaigns

SOLUTION:

Please refer to the CVE-2021-43890 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43890).

Workaround:Option1: Enable the following GPO to prevent non-admins from installing any Windows App packages.

BlockNonAdminUserInstall- This policy setting manages the ability of non-administrator users to install (signed) Windows app packages. When enabled (value: 1), non-administrator users will be unable to initiate the installation of (signed) Windows app packages.

Option2: Enable this GPO to prevent installing apps from outside the Microsoft Store
AllowAllTrustedAppToInstall- This policy setting allows you to manage the installation of trusted line-of-business (LOB) or developer-signed Windows Store apps.If you enable this policy setting, you can install any LOB or developer-signed Windows Store app (which must be signed with a certificate chain that can be successfully validated by the local computer)

Option3: Disable the ms-appinstaller protocol to install apps directly from a website.
ms-appinstaller- This will block all attempts to invoke the protocol from the browser. Specifically, how that looks to the user will depend on the construction of the page that tries to launch the protocol.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-43890 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43890)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Qualys
- Reference: CVE-2021-43890
- Description: By abusing the ms-appinstaller:// URI handler in Microsoft Windows, one can trick users into thinking that the website is trying to ask them to install software to do something
- Link: https://attackerkb.com/topics/fuXBLecKVt/cve-2021-43890

cisa-kev
- Reference: CVE-2021-43890
- Description: Microsoft Windows AppX Installer Spoofing Vulnerability
- Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

nist-nvd2
- Reference: CVE-2021-43890
- Description: We have investigated reports of a spoofing vulnerability in AppX installer that affects Microsoft Windows. Microsoft is aware of attacks that attempt to exploit this vulnerability by using specially crafted packages that include the malware family known as Emotet/Trickbot/Bazaloader.
  An attacker could craft a malicious attachment to be used in phishing campaigns. The attacker would then have to convince the user to open the specially crafted attachment. Users whose accounts are configured to hav
- Link: https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/

microsoft-cvrf
- Reference: CVE-2021-43890
- Description: Windows AppX Installer Spoofing Vulnerability
- Link: https://api.msrc.microsoft.com/cvrf/2021-Dec?api-version=2020

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Policies\Microsoft\Windows\Appx BlockNonAdminUserInstall is missing.
HKLM\SOFTWARE\Policies\Microsoft\Windows\Appx AllowAllTrustedApps is missing.
HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\Appx BlockNonAdminUserInstall is missing.
HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\Appx AllowAllTrustedApps is missing.
Microsoft vulnerable Microsoft Desktop Installer detected

Version '1.0.30251.0'

4 Microsoft Windows Codecs Library HEVC Video and VP9 Extensions Remote Code Execution (RCE) Vulnerability for February 2022

QID:	91866
Category:	Windows
Associated CVEs:	CVE-2022-22709, CVE-2022-21927, CVE-2022-21926, CVE-2022-21844
Vendor Reference:	CVE-2022-22709, CVE-2022-21927, CVE-2022-21926, CVE-2022-21844
Bugtraq ID:	-
Service Modified:	02/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory.

Affected Product:
"HEVC from Device Manufacturer" media codec before version 1.0.43421.0
"VP9 from Device Manufacturer" media codec before version 1.0.42791.0

IMPACT:

An attacker who successfully exploited this vulnerability can compromise confidentiality, integrity and availability of the system

SOLUTION:

Users are advised to check CVE-2022-22709 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22709)
CVE-2022-21927 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21927)
CVE-2022-21926 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21926) and
CVE-2022-21844 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21844)

for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2022-22709 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22709)

CVE-2022-21927 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21927)

CVE-2022-21926 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21926)

CVE-2022-21844 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21844)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'

4 Microsoft Windows Codecs Library Remote Code Execution (RCE) Vulnerability for March 2022

QID:	91869
Category:	Windows
Associated CVEs:	CVE-2022-23300, CVE-2022-22007, CVE-2022-23301, CVE-2022-24451, CVE-2022-24452, CVE-2022-24453, CVE-2022-24457, CVE-2022-23295, CVE-2022-22006, CVE-2022-24501, CVE-2022-24456
Vendor Reference:	CVE-2022-23301, CVE-2022-24451, CVE-2022-24452, CVE-2022-24453, CVE-2022-24457, CVE-2022-23295, CVE-2022-22006, CVE-2022-24501, CVE-2022-24456, CVE-2022-22007, CVE-2022-23300
Bugtraq ID:	-
Service Modified:	04/26/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Multiple security vulnerabilities exist in Microsoft Windows Codecs Library.

Affected Product:
HEIFImageExtension before 1.0.43012.0
VP9VideoExtensions before 1.0.42791.0
HEVCVideoExtension before 1.0.50361.0 and 1.0.50362.0
For Windows 11 RawImageExtension before 2.1.30391.0
For Windows 10 RawImageExtension before 2.0.30391.0

IMPACT:

An attacker who successfully exploited the vulnerability could execute arbitrary code.

SOLUTION:

Users are advised to check CVE-2022-23300 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23300)
Users are advised to check CVE-2022-23295 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23295)
Users are advised to check CVE-2022-22007 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22007)
Users are advised to check CVE-2022-23301 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23301)
Users are advised to check CVE-2022-24451 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24451)
Users are advised to check CVE-2022-24452 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24452)
Users are advised to check CVE-2022-24453 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24453)
Users are advised to check CVE-2022-24457 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24457)
Users are advised to check CVE-2022-22006 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006)
Users are advised to check CVE-2022-24501 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501)
Users are advised to check CVE-2022-24456 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24456)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2022-23300 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23300)

CVE-2022-23295 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23295)

CVE-2022-22007 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23307)

CVE-2022-23301 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23301)

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

CVE-2022-24452 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24452)

CVE-2022-24453 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24453)

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

CVE-2022-22006 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006)

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

CVE-2022-24456 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24456)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'
Microsoft vulnerable Microsoft.HEIFImageExtension detected
Version '1.0.22742.0'

4 Microsoft Photos App Remote Code Execution (RCE) Vulnerability for June 2022

QID:	91914
Category:	Windows
Associated CVEs:	CVE-2022-30168
Vendor Reference:	CVE-2022-30168
Bugtraq ID:	-
Service Modified:	07/16/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Photos is a single-instance app that can organize digital photos in its gallery into albums.

CVE-2022-30168: Microsoft Photos App Remote Code Execution Vulnerability

Affected Versions:
Microsoft Photos App prior to version 2022.30050.31008.0

IMPACT:

A successful exploit of this vulnerability could lead to execute remote code execution on a machine.

SOLUTION:

Users are advised to check CVE-2022-30168 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30168) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2022-30168 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30168)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.Windows.Photos detected
Version '2019.19071.12548.0'

4 Microsoft Defender Denial of Service (DoS) Vulnerability for April 2023

QID:	92008
Category:	Windows
Associated CVEs:	CVE-2023-24860, CVE-2023-24934
Vendor Reference:	CVE-2023-24934, CVE-2023-24860

Bugtraq ID:	-
Service Modified:	04/14/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.

Affected Versions / Software:
Microsoft Malware Protection Engine version prior to Version 1.1.20200.4

IMPACT:

Successful exploitation of this vulnerability could lead to Denial of Service Vulnerability

SOLUTION:

Users are advised to check CVE-2023-24860 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24860), CVE-2023-24934 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24934) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-24860 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24860)

CVE-2023-24934 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24934)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

4 Microsoft Paint 3D Remote Code Execution (RCE) Vulnerability for July 2023

QID:	92032
Category:	Windows
Associated CVEs:	CVE-2023-32047, CVE-2023-35374
Vendor Reference:	CVE-2023-32047, CVE-2023-35374
Bugtraq ID:	-
Service Modified:	03/04/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Paint 3D is prone to Remote Code Execution Vulnerability.

Affected Product:
Microsoft Paint 3D prior to 6.2305.16087.0

IMPACT:

Successful exploitation of the vulnerability may allow remote code execution leading to complete system compromise.

SOLUTION:

Users are advised to refer to CVE-2023-32047 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32047) CVE-2023-35374 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35374) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-32047 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32047)

CVE-2023-35374 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35374)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable Microsoft Paint 3D detected via App store:wmi query select version from Win32_InstalledStoreProgram where name='Microsoft.MSPaint'
Version '6.1907.29027.0'

 4 Microsoft Defender Elevation of Privilege Vulnerability for July 2023

QID:	92039
Category:	Windows
Associated CVEs:	CVE-2023-33156
Vendor Reference:	CVE-2023-33156
Bugtraq ID:	-
Service Modified:	07/14/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.

Affected Versions / Software:
Microsoft Malware Protection Engine version prior to Version 1.1.23050.3

IMPACT:

Successful exploitation of this vulnerability requires an attacker to win a race condition.

SOLUTION:

Users are advised to check CVE-2023-33156 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33156) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-33156 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33156)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

4 Microsoft Windows Defender Attack Surface Reduction Security Feature Bypass Vulnerability for September 2023

QID:	92058
Category:	Windows
Associated CVEs:	CVE-2023-38163
Vendor Reference:	CVE-2023-38163
Bugtraq ID:	-
Service Modified:	09/14/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Defender is prone to Attack Surface Reduction Security Feature Bypass Vulnerability

Affected Software:
Microsoft Defender Security Intelligence Updates

Affected Version:
Windows Defender prior to build 1.391.1332.0

IMPACT:

An attacker who successfully exploited this vulnerability could bypass the Windows Defender Attack Surface Reduction blocking feature.

SOLUTION:

Users are advised to check CVE-2023-38163 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38163) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-38163 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38163)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

4 Microsoft 3D Viewer Remote Code Execution (RCE) Vulnerability - September 2023

QID:	92061
Category:	Windows
Associated CVEs:	CVE-2023-36739, CVE-2023-36740, CVE-2023-36760
Vendor Reference:	CVE-2023-36739, CVE-2023-36740, CVE-2023-36760
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-

Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft 3D Viewer is prone to Remote Code Execution Vulnerability.

Affected Versions:
Microsoft 3D-Viewer App package versions prior to 7.2306.12012.0

IMPACT:

Successful exploitation allows an attacker to execute code remotely.

SOLUTION:

Users are advised to check CVE-2023-36739 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36739),CVE-2023-36740 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36740) for more information.

,CVE-2023-36760 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36760) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-36739 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36739)

CVE-2023-36740 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36740)

CVE-2023-36760 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36760)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.Microsoft3DViewer detected
Version '6.1908.2042.0'

4 Microsoft Windows Defender Elevation of Privilege Vulnerability for November 2023

QID:	92079
Category:	Windows
Associated CVEs:	CVE-2023-36422
Vendor Reference:	CVE-2023-36422
Bugtraq ID:	-
Service Modified:	12/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Defender Antivirus (formerly Windows Defender) is an antivirus software component of Microsoft Windows.

Successful exploitation of this vulnerability could allow a local attacker to execute code with SYSTEM privileges.

Affected Software:
Microsoft Malware Protection Engine version prior to Version 1.1.23100.2009

IMPACT:

A local attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

SOLUTION:

Customers are advised to follow CVE-2023-36422 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36422) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-36422 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36422)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

4 Microsoft Defender Denial of Service (DoS) Vulnerability For December 2023

QID:	92084
Category:	Windows
Associated CVEs:	CVE-2023-36010
Vendor Reference:	CVE-2023-36010
Bugtraq ID:	-
Service Modified:	04/03/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Malware Protection Platform is affected by a denial of service vulnerability CVE-2023-36010.

Affected Versions / Software:
Microsoft Malware Protection Platform prior to Version 4.18.23110.3

IMPACT:

Successful exploitation of this vulnerability could lead to Denial of Service Vulnerability

SOLUTION:

Users are advised to check CVE-2023-36010 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36010) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-36010 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36010)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files\Windows Defender\\ProtectionManagement.dll Version is 4.18.1909.6

4 Microsoft .NET Framework Update for January 2024

QID:	92097
Category:	Windows
Associated CVEs:	CVE-2024-0056, CVE-2024-21312, CVE-2024-0057, CVE-2023-36042
Vendor Reference:	5034280, 5034270, 5033920, 5034272, 5034275, 5034274, 5034276, 5034279, 5034278, 5034269, 5034119, 5034273, 5034277, 5033910
Bugtraq ID:	-
Service Modified:	01/17/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A Denial of Service Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
5034280
5034270
5033920
5034272
5034275
5034274
5034276
5034279
5034278
5034269
5034119
5034273
5034277
5033910

This security update is rated Important for supported versions of Microsoft .NET Framework.
.NET Framework 2.0, 3.0, 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation may allow a attacker to perform Denial of Service.

SOLUTION:

Customers are advised to refer to CVE-2024-0056 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056), CVE-2024-21312 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312), CVE-2024-0057 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057) for more details pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-0056 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056)

CVE-2024-21312 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312)

CVE-2024-0057 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5034275 or KB5034274 or KB5034276 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.dll Version is 4.8.4682.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.dll Version is 4.8.4682.0

4 Microsoft 3D Viewer Remote Code Execution (RCE) Vulnerability - February 2024

QID:	92117
Category:	Windows
Associated CVEs:	CVE-2024-20677
Vendor Reference:	CVE-2024-20677
Bugtraq ID:	-
Service Modified:	02/20/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft 3D Viewer is prone to Remote Code Execution Vulnerability.

Affected Versions:
Microsoft 3D-Viewer App package versions prior to 7.2401.29012.0

IMPACT:

Successful exploitation allows an attacker to execute code remotely.

SOLUTION:

Users are advised to check CVE-2024-20677 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-20677 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.Microsoft3DViewer detected
Version '6.1908.2042.0'

4 Microsoft Windows Security Update for March 2024

QID:	92121
Category:	Windows
Associated CVEs:	CVE-2024-21407, CVE-2024-21408, CVE-2024-21427, CVE-2024-21431, CVE-2024-21432, CVE-2024-21436, CVE-2024-21440, CVE-2024-21444, CVE-2024-21445, CVE-2024-21446, CVE-2024-21450, CVE-2024-26159, CVE-2024-26160, CVE-2024-26162, CVE-2024-26166, CVE-2024-26169, CVE-2024-26173, CVE-2024-26176, CVE-2024-26177, CVE-2024-26178,

	CVE-2024-26181, CVE-2024-26182, CVE-2024-26185, CVE-2024-26190, CVE-2024-21429, CVE-2024-21430, CVE-2024-21433, CVE-2024-21434, CVE-2024-21435, CVE-2024-21437, CVE-2024-21438, CVE-2024-21439, CVE-2024-21441, CVE-2024-21442, CVE-2024-21443, CVE-2024-21451, CVE-2024-26174, CVE-2023-28746, CVE-2024-26161, CVE-2024-26197, CVE-2024-26170
Vendor Reference:	KB5035849, KB5035857, KB5035854, KB5035845, KB5035853, KB5035856, KB5035858, KB5035855, KB5035930, KB5035885, KB5035920, KB5035933, KB5035888, KB5035919
Bugtraq ID:	-
Service Modified:	08/26/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - March 2024

Patch version is 10.0.17763.5576 for KB5035849 (https://support.microsoft.com/en-in/help/5035849)
Patch version is for 10.0.20348.2340 KB5035857 (https://support.microsoft.com/en-in/help/5035857)
Patch version is for 10.0.22000.2836 KB5035854 (https://support.microsoft.com/en-in/help/5035854)
Patch version is for 10.0.19041.4170 KB5035845 (https://support.microsoft.com/en-in/help/5035845)
Patch version is for 10.0.22621.3296 KB5035853 (https://support.microsoft.com/en-in/help/5035853)
Patch version is for 10.0.25398.763 KB5035856 (https://support.microsoft.com/en-in/help/5035856)
Patch version is for 10.0.10240.20526 KB5035858 (https://support.microsoft.com/en-in/help/5035858)
Patch version is for 10.0.14393.6795 KB5035855 (https://support.microsoft.com/en-in/help/5035855)
Patch version is for 6.2.9200.24768 KB5035930 (https://support.microsoft.com/en-in/help/5035930)
Patch version is for 6.3.9600.21871 KB5035885 (https://support.microsoft.com/en-in/help/5035885)
Patch version is for 6.0.6003.22567 KB5035920 (https://support.microsoft.com/en-in/help/5035920)
Patch version is for 6.0.6003.22567 KB5035933 (https://support.microsoft.com/en-in/help/5035933)
Patch version is for 6.1.7601.27017 KB5035888 (https://support.microsoft.com/en-in/help/5035888)
Patch version is for 6.1.7601.27017 KB5035919 (https://support.microsoft.com/en-in/help/5035919)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5035849 (https://support.microsoft.com/en-in/help/5035849)
KB5035857 (https://support.microsoft.com/en-in/help/5035857)
KB5035854 (https://support.microsoft.com/en-in/help/5035854)
KB5035845 (https://support.microsoft.com/en-in/help/5035845)
KB5035853 (https://support.microsoft.com/en-in/help/5035853)
KB5035856 (https://support.microsoft.com/en-in/help/5035856)
KB5035858 (https://support.microsoft.com/en-in/help/5035858)
KB5035855 (https://support.microsoft.com/en-in/help/5035855)
KB5035930 (https://support.microsoft.com/en-in/help/5035930)
KB5035885 (https://support.microsoft.com/en-in/help/5035885)
KB5035920 (https://support.microsoft.com/en-in/help/5035920)
KB5035933 (https://support.microsoft.com/en-in/help/5035933)
KB5035888 (https://support.microsoft.com/en-in/help/5035888)
KB5035919 (https://support.microsoft.com/en-in/help/5035919)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

5035849 (https://support.microsoft.com/en-in/help/5035849)

5035857 (https://support.microsoft.com/en-in/help/5035857)

5035854 (https://support.microsoft.com/en-in/help/5035854)

5035845 (https://support.microsoft.com/en-in/help/5035845)

5035853 (https://support.microsoft.com/en-in/help/5035853)

5035856 (https://support.microsoft.com/en-in/help/5035856)

5035858 (https://support.microsoft.com/en-in/help/5035858)

5035855 (https://support.microsoft.com/en-in/help/5035855)

5035930 (https://support.microsoft.com/en-in/help/5035930)

5035885 (https://support.microsoft.com/en-in/help/5035885)

5035920 (https://support.microsoft.com/en-in/help/5035920)

5035933 (https://support.microsoft.com/en-in/help/5035933)

5035888 (https://support.microsoft.com/en-in/help/5035888)

5035919 (https://support.microsoft.com/en-in/help/5035919)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference:	CVE-2024-26182
Description:	Windows Kernel Subkey List Use-After-Free
Link:	https://packetstormsecurity.com/files/178012/Windows-Kernel-Subkey-List-Use-After-Free.html

cisa-kev

Reference:	CVE-2024-26169
Description:	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability
Link:	https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	CVE-2024-26169
Type:	Exploit
Platform:	Win64

RESULTS:

KB5035845 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

4 Microsoft Windows Security Update for May 2024

QID:	92139
Category:	Windows
Associated CVEs:	CVE-2024-29996, CVE-2024-29997, CVE-2024-29998, CVE-2024-29999, CVE-2024-30000, CVE-2024-30001, CVE-2024-30002, CVE-2024-30003, CVE-2024-30004, CVE-2024-30005, CVE-2024-30006, CVE-2024-30007, CVE-2024-30008, CVE-2024-30009, CVE-2024-30010, CVE-2024-30011, CVE-2024-30012, CVE-2024-30014, CVE-2024-30015, CVE-2024-30016, CVE-2024-30017, CVE-2024-30018, CVE-2024-30019, CVE-2024-30020, CVE-2024-30021, CVE-2024-30022, CVE-2024-30023, CVE-2024-26238, CVE-2024-29994, CVE-2024-30024, CVE-2024-30025, CVE-2024-30027, CVE-2024-30028, CVE-2024-30029, CVE-2024-30030, CVE-2024-30031, CVE-2024-30032, CVE-2024-30033, CVE-2024-30034, CVE-2024-30035, CVE-2024-30036, CVE-2024-30037, CVE-2024-30038, CVE-2024-30039, CVE-2024-30049, CVE-2024-30051, CVE-2024-30040, CVE-2024-30050
Vendor Reference:	KB5037765, KB5037782, KB5037770, KB5037768, KB5037771, KB5037781, KB5037788, KB5037763, KB5037800, KB5037836, KB5037780, KB5037803, KB5037778, KB5037823
Bugtraq ID:	-
Service Modified:	09/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - May 2024

KB5037765 (https://support.microsoft.com/en-in/help/5037765)
KB5037782 (https://support.microsoft.com/en-in/help/5037782)
KB5037770 (https://support.microsoft.com/en-in/help/5037770)
KB5037768 (https://support.microsoft.com/en-in/help/5037768)

KB5037771 (https://support.microsoft.com/en-in/help/5037771)
KB5037781 (https://support.microsoft.com/en-in/help/5037781)
KB5037788 (https://support.microsoft.com/en-in/help/5037788)
KB5037763 (https://support.microsoft.com/en-in/help/5037763)
KB5037800 (https://support.microsoft.com/en-in/help/5037800)
KB5037836 (https://support.microsoft.com/en-in/help/5037836)
KB5037780 (https://support.microsoft.com/en-in/help/5037780)
KB5037803 (https://support.microsoft.com/en-in/help/5037803)
KB5037778 (https://support.microsoft.com/en-in/help/5037778)
KB5037823 (https://support.microsoft.com/en-in/help/5037823)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5037765 (https://support.microsoft.com/en-in/help/5037765)
KB5037782 (https://support.microsoft.com/en-in/help/5037782)
KB5037770 (https://support.microsoft.com/en-in/help/5037770)
KB5037768 (https://support.microsoft.com/en-in/help/5037768)
KB5037771 (https://support.microsoft.com/en-in/help/5037771)
KB5037781 (https://support.microsoft.com/en-in/help/5037781)
KB5037788 (https://support.microsoft.com/en-in/help/5037788)
KB5037763 (https://support.microsoft.com/en-in/help/5037763)
KB5037800 (https://support.microsoft.com/en-in/help/5037800)
KB5037836 (https://support.microsoft.com/en-in/help/5037836)
KB5037780 (https://support.microsoft.com/en-in/help/5037780)
KB5037803 (https://support.microsoft.com/en-in/help/5037803)
KB5037778 (https://support.microsoft.com/en-in/help/5037778)
KB5037823
(https://support.microsoft.com/en-in/help/5037823)Workaround:https://support.microsoft.com/en-us/topic/may-23-2024-kb5039705-os-build-17763-5830-out-of-band-2285667a-13a3-4fd9-98a0-e980eb996aac

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5037763 (https://support.microsoft.com/en-in/help/5037763)

KB5037765 (https://support.microsoft.com/en-in/help/5037765)

KB5037768 (https://support.microsoft.com/en-in/help/5037768)

KB5037770 (https://support.microsoft.com/en-in/help/5037770)

KB5037771 (https://support.microsoft.com/en-in/help/5037771)

KB5037778 (https://support.microsoft.com/en-in/help/5037778)

KB5037780 (https://support.microsoft.com/en-in/help/5037778)

KB5037781 (https://support.microsoft.com/en-in/help/5037781)

KB5037782 (https://support.microsoft.com/en-in/help/5037782)

KB5037788 (https://support.microsoft.com/en-in/help/5037788)

KB5037800 (https://support.microsoft.com/en-in/help/5037800)

KB5037803 (https://support.microsoft.com/en-in/help/5037803)

KB5037823 (https://support.microsoft.com/en-in/help/5037823)

KB5037836 (https://support.microsoft.com/en-in/help/5037836)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference:	CVE-2024-30038
Description:	Microsoft Windows TOCTOU Local Privilege Escalation
Link:	https://packetstormsecurity.com/files/181593/Microsoft-Windows-TOCTOU-Local-Privilege-Escalation.html

Reference:	CVE-2024-30051
Description:	Microsoft Windows DWM Core Library Privilege Escalation
Link:	https://packetstormsecurity.com/files/181402/Microsoft-Windows-DWM-Core-Library-Privilege-Escalation.html

metasploit
Reference: CVE-2024-30038
Description: Windows Kernel Time of Check Time of Use LPE in AuthzBasepCopyoutInternalSecurityAttributes
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/local/cve_2024_30088_authz_base

0day.today
Reference: CVE-2024-30038
Description: Microsoft Windows TOCTOU Local Privilege Escalation Exploit
Link: https://0day.today/exploit/39753

github-exploits
Reference: CVE-2024-30051
Description: fortra/CVE-2024-30051 exploit repository
Link: https://github.com/fortra/CVE-2024-30051

cisa-kev
Reference: CVE-2024-30040
Description: Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-30051
Description: Microsoft DWM Core Library Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2024-30051
Description: Windows Kernel Heap overflow in DWM Core
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs
Reference: CVE-2024-26238
Description: WINDOWS 10 PLUGSCHEDULER ELEVATION OF PRIVILEGE
Link: https://www.synacktiv.com/advisories/windows-10-plugscheduler-elevation-of-privilege

Reference: CVE-2024-30051
Description: A public secret : Research on the CVE-2024-30051 privilege escalation vulnerability in the wild
Link: https://ti.qianxin.com/blog/articles/public-secret-research-on-the-cve-2024-30051-privilege-escalation-vulnerability-in-the-wild-en/

Reference: CVE-2024-30051
Description: Windows DWM Core Library Elevation of Privilege Vulnerability (CVE-2024-30051)
Link: https://www.coresecurity.com/core-labs/articles/windows-dwm-core-library-elevation-privilege-vulnerability-cve-2024-30051

microsoft-cvrf
Reference: CVE-2024-30040
Description: Windows MSHTML Platform Security Feature Bypass Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-May?api-version=2020

Reference: CVE-2024-30051
Description: Windows DWM Core Library Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-May?api-version=2020

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2024-30051
Type: Exploit
Platform: Document,Win64

RESULTS:

KB5037768 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

4 Microsoft Windows Security Update for June 2024

QID:	92142
Category:	Windows
Associated CVEs:	CVE-2024-30099, CVE-2024-30097, CVE-2024-30096, CVE-2024-35265, CVE-2024-30095, CVE-2024-30094, CVE-2024-30093, CVE-2024-30091, CVE-2024-30090, CVE-2024-30089, CVE-2024-30088, CVE-2024-30087, CVE-2024-30086, CVE-2024-30085, CVE-2024-30084, CVE-2024-30083, CVE-2024-30068, CVE-2024-30067, CVE-2024-30066, CVE-2024-30065, CVE-2024-30064, CVE-2024-30063, CVE-2024-30062, CVE-2023-50868, CVE-2024-35250, CVE-2024-30082, CVE-2024-30080, CVE-2024-30078, CVE-2024-30077, CVE-2024-30076, CVE-2024-30075, CVE-2024-30074, CVE-2024-30072, CVE-2024-30070, CVE-2024-30069, CVE-2024-38213
Vendor Reference:	KB5039214, KB5039225, KB5039236, KB5039212, KB5039211, KB5039213, KB5039227, KB5039217, KB5039294, KB5039260, KB5039289, KB5039274, KB5039245, KB5039266
Bugtraq ID:	-
Service Modified:	09/07/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - May 2024

KB5039214 (https://support.microsoft.com/en-in/help/5039214)
KB5039225 (https://support.microsoft.com/en-in/help/5039225)
KB5039236 (https://support.microsoft.com/en-in/help/5039236)
KB5039212 (https://support.microsoft.com/en-in/help/5039212)
KB5039211 (https://support.microsoft.com/en-in/help/5039211)
KB5039213 (https://support.microsoft.com/en-in/help/5039213)
KB5039227 (https://support.microsoft.com/en-in/help/5039227)
KB5039217 (https://support.microsoft.com/en-in/help/5039217)
KB5039294 (https://support.microsoft.com/en-in/help/5039294)
KB5039260 (https://support.microsoft.com/en-in/help/5039260)
KB5039289 (https://support.microsoft.com/en-in/help/5039289)
KB5039274 (https://support.microsoft.com/en-in/help/5039274)
KB5039245 (https://support.microsoft.com/en-in/help/5039245)
KB5039266 (https://support.microsoft.com/en-in/help/5039266)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5039214 (https://support.microsoft.com/en-in/help/5039214)
KB5039225 (https://support.microsoft.com/en-in/help/5039225)
KB5039236 (https://support.microsoft.com/en-in/help/5039236)
KB5039212 (https://support.microsoft.com/en-in/help/5039212)
KB5039211 (https://support.microsoft.com/en-in/help/5039211)
KB5039213 (https://support.microsoft.com/en-in/help/5039213)
KB5039227 (https://support.microsoft.com/en-in/help/5039227)
KB5039217 (https://support.microsoft.com/en-in/help/5039217)
KB5039294 (https://support.microsoft.com/en-in/help/5039294)
KB5039260 (https://support.microsoft.com/en-in/help/5039260)
KB5039289 (https://support.microsoft.com/en-in/help/5039289)
KB5039274 (https://support.microsoft.com/en-in/help/5039274)
KB5039245 (https://support.microsoft.com/en-in/help/5039245)
KB5039266 (https://support.microsoft.com/en-in/help/5039266)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5039214 (https://support.microsoft.com/en-in/help/5039214)

KB5039235 (https://support.microsoft.com/en-in/help/5039225)

KB5039236 (https://support.microsoft.com/en-in/help/5039236)

KB5039212 (https://support.microsoft.com/en-in/help/5039212)

KB5039211 (https://support.microsoft.com/en-in/help/5039211)

KB5039213 (https://support.microsoft.com/en-in/help/5039213)

KB5039227 (https://support.microsoft.com/en-in/help/5039227)

KB5039217 (https://support.microsoft.com/en-in/help/5039217)

KB5039294 (https://support.microsoft.com/en-in/help/5039294)

KB5039260 (https://support.microsoft.com/en-in/help/5039260)

KB5039289 (https://support.microsoft.com/en-in/help/5039289)

KB5039274 (https://support.microsoft.com/en-in/help/5039274)

KB5039245 (https://support.microsoft.com/en-in/help/5039245)

KB5039266 (https://support.microsoft.com/en-in/help/5039266)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2024-30088
Description: Collateral Damage CVE-2024-30088 Privilege Escalation
Link: https://packetstormsecurity.com/files/179642/Collateral-Damage-CVE-2024-30088-Privilege-Escalation.html

github-exploits

Reference: CVE-2024-30088
Description: exploits-forsale/collateral-damage exploit repository
Link: https://github.com/exploits-forsale/collateral-damage

Reference: CVE-2024-30088
Description: tykawaii98/CVE-2024-30088 exploit repository
Link: https://github.com/tykawaii98/CVE-2024-30088

Reference: CVE-2024-30088
Description: Zombie-Kaiser/CVE-2024-30088-Windows-poc exploit repository
Link: https://github.com/Zombie-Kaiser/CVE-2024-30088-Windows-poc

Reference: CVE-2024-30088
Description: NextGenPentesters/CVE-2024-30088- exploit repository
Link: https://github.com/NextGenPentesters/CVE-2024-30088-

Reference: CVE-2024-30088
Description: Admin9961/CVE-2024-30088 exploit repository
Link: https://github.com/Admin9961/CVE-2024-30088

cisa-kev

Reference: CVE-2024-38213
Description: Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

gist

Reference: CVE-2024-30088
Description: CVE-2024-30088 PoC
Link: https://gist.github.com/carrot-c4k3/6ef33d57733b08281b26db0a50b1a447

blogs

Reference: CVE-2024-30080
Description: SIMPLE ANALYZE ABOUT CVE-2024-30080
Link: https://whereisk0shl.top/post/simple-analyze-about-cve-2024-30080

Reference: CVE-2024-30078

Description: Windows Wi-Fi Driver RCE Vulnerability - CVE-2024-30078
Link: https://www.crowdfense.com/windows-wi-fi-driver-rce-vulnerability-cve-2024-30078/

microsoft-cvrf
Reference: CVE-2024-38213
Description: Windows Mark of the Web Security Feature Bypass Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Aug?api-version=2020

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5039211 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

4 Microsoft Windows App Installer Spoofing Vulnerability for August 2024

QID:	92163
Category:	Windows
Associated CVEs:	CVE-2024-38177
Vendor Reference:	CVE-2024-38177
Bugtraq ID:	-
Service Modified:	08/17/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

CVE-2024-38177: Windows App Installer Spoofing Vulnerability

IMPACT:

An attacker could craft a malicious attachment to be used in phishing campaigns

SOLUTION:

Please refer to the CVE-2024-38177 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38177).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-38177 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38177)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft Desktop Installer detected
Version '1.0.30251.0'

4 Microsoft Windows Security Update for September 2024

QID:	92169
Category:	Windows
Associated CVEs:	CVE-2024-38119, CVE-2024-38230, CVE-2024-38236, CVE-2024-38240, CVE-2024-38241, CVE-2024-38242, CVE-2024-38249, CVE-2024-38250, CVE-2024-38252, CVE-2024-38253, CVE-2024-38254, CVE-2024-38256, CVE-2024-43467, CVE-2024-38014, CVE-2024-38046, CVE-2024-38217, CVE-2024-38231, CVE-2024-38232, CVE-2024-38233, CVE-2024-38234, CVE-2024-38235, CVE-2024-38237, CVE-2024-38238, CVE-2024-38239, CVE-2024-38243, CVE-2024-38244, CVE-2024-38245, CVE-2024-38246, CVE-2024-38247, CVE-2024-38248, CVE-2024-38257, CVE-2024-38258, CVE-2024-38259, CVE-2024-38260, CVE-2024-38263, CVE-2024-21416, CVE-2024-38045, CVE-2024-43454, CVE-2024-43455, CVE-2024-43457, CVE-2024-43458, CVE-2024-43461, CVE-2024-43475, CVE-2024-30073, CVE-2024-43495, CVE-2024-43487
Vendor Reference:	KB5040438, KB5040442, KB5043050, KB5042881, KB5042880, KB5043067, KB5043064, KB5043076, KB5043080, KB5043083, KB5043051, KB5043055, KB5043138, KB5043135, KB5043087, KB5043129, KB5043092, KB5043125, KB5043049
Bugtraq ID:	-
Service Modified:	09/18/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows Security Update - September 2024

KB5043050 (https://support.microsoft.com/en-in/help/5043050)
KB5042881 (https://support.microsoft.com/en-in/help/5042881)
KB5042880 (https://support.microsoft.com/en-in/help/5042880)
KB5043067 (https://support.microsoft.com/en-in/help/5043067)
KB5043064 (https://support.microsoft.com/en-in/help/5043064)
KB5043076 (https://support.microsoft.com/en-in/help/5043076)
KB5043080 (https://support.microsoft.com/en-in/help/5043080)
KB5043083 (https://support.microsoft.com/en-in/help/5043083)
KB5043051 (https://support.microsoft.com/en-in/help/5043051)
KB5043055 (https://support.microsoft.com/en-in/help/5043055)
KB5043138 (https://support.microsoft.com/en-in/help/5043138)
KB5043135 (https://support.microsoft.com/en-in/help/5043135)
KB5043087 (https://support.microsoft.com/en-in/help/5043087)
KB5043129 (https://support.microsoft.com/en-in/help/5043129)
KB5043092 (https://support.microsoft.com/en-in/help/5043092)
KB5043125 (https://support.microsoft.com/en-in/help/5043125)
KB5043049 (https://support.microsoft.com/en-in/help/5043049)
KB5040442 (https://support.microsoft.com/en-in/help/5040442)
KB5040438 (https://support.microsoft.com/en-in/help/5040438)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5043050 (https://support.microsoft.com/en-in/help/5043050)
KB5042881 (https://support.microsoft.com/en-in/help/5042881)
KB5042880 (https://support.microsoft.com/en-in/help/5042880)
KB5043067 (https://support.microsoft.com/en-in/help/5043067)
KB5043064 (https://support.microsoft.com/en-in/help/5043064)
KB5043076 (https://support.microsoft.com/en-in/help/5043076)
KB5043080 (https://support.microsoft.com/en-in/help/5043080)
KB5043083 (https://support.microsoft.com/en-in/help/5043083)
KB5043051 (https://support.microsoft.com/en-in/help/5043051)
KB5043055 (https://support.microsoft.com/en-in/help/5043055)
KB5043138 (https://support.microsoft.com/en-in/help/5043138)
KB5043135 (https://support.microsoft.com/en-in/help/5043135)
KB5043087 (https://support.microsoft.com/en-in/help/5043087)
KB5043129 (https://support.microsoft.com/en-in/help/5043129)
KB5043092 (https://support.microsoft.com/en-in/help/5043092)
KB5043125 (https://support.microsoft.com/en-in/help/5043125)

KB5043049 (https://support.microsoft.com/en-in/help/5043049)
KB5040442 (https://support.microsoft.com/en-in/help/5040442)
KB5040438 (https://support.microsoft.com/en-in/help/5040438)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5043050 (https://support.microsoft.com/en-in/help/5043050)

KB5042881 (https://support.microsoft.com/en-in/help/5042881)

KB5042880 (https://support.microsoft.com/en-in/help/5042880)

KB5043067 (https://support.microsoft.com/en-in/help/5043067)

KB5043064 (https://support.microsoft.com/en-in/help/5043064)

KB5043076 (https://support.microsoft.com/en-in/help/5043076)

KB5043080 (https://support.microsoft.com/en-in/help/5043080)

KB5043083 (https://support.microsoft.com/en-in/help/5043083)

KB5043051 (https://support.microsoft.com/en-in/help/5043051)

KB5043055 (https://support.microsoft.com/en-in/help/5043055)

KB5043138 (https://support.microsoft.com/en-in/help/5043138)

KB5043135 (https://support.microsoft.com/en-in/help/5043135)

KB5043087 (https://support.microsoft.com/en-in/help/5043087)

KB5043129 (https://support.microsoft.com/en-in/help/5043129)

KB5043092 (https://support.microsoft.com/en-in/help/5043092)

KB5043125 (https://support.microsoft.com/en-in/help/5043125)

KB5043049 (https://support.microsoft.com/en-in/help/5043049)

KB5040442 (https://support.microsoft.com/en-in/help/5040442)

KB5040438 (https://support.microsoft.com/en-in/help/5040438)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

cisa-kev

Reference: CVE-2024-43461
Description: Microsoft Windows MSHTML Platform Spoofing Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-38014
Description: Microsoft Windows Installer Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2024-38217
Description: Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

blogs

Reference: CVE-2024-38014
Description: Microsoft Windows MSI Installer - Repair to SYSTEM - A detailed journey
Link: https://sec-consult.com/blog/detail/msi-installer-repair-to-system-a-detailed-journey/

microsoft-cvrf

Reference: CVE-2024-43461
Description: Windows MSHTML Platform Spoofing Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Sep?api-version=2020

Reference: CVE-2024-38014
Description: Windows Installer Elevation of Privilege Vulnerability
Link: https://api.msrc.microsoft.com/cvrf/2024-Sep?api-version=2020

Reference: CVE-2024-38217
Description: Windows Mark of the Web Security Feature Bypass Vulnerability

Link: https://api.msrc.microsoft.com/cvrf/2024-Sep?api-version=2020

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5043064 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

4 VLC Player DLL Preloading Code Execution Vulnerability (VideoLAN-SA-1005)

QID:	118441
Category:	Local
Associated CVEs:	CVE-2010-3124
Vendor Reference:	VideoLAN-SA-1005
Bugtraq ID:	-
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

Due to the DLL loading design on Windows, VLC automatically loads a DLL from the current directory, if it doesn't find it in VLC's application directory or in system directories.

Affected Versions:
All VLC Media Player Versions up to 1.1.3

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to execute arbitrary code in context of VLC media player.

SOLUTION:

VLC media player 1.1.4 addresses this issue.

Refer to vendor advisory VideoLAN-SA-1005 (http://www.videolan.org/security/sa1005.html) to obtain additional details about the vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1005: Windows (VLC Media Player 1.1.4) (http://sourceforge.net/projects/vlc/files/1.1.4/win32/vlc-1.1.4-win32.exe/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2010-3124
Description: VideoLAN VLC Media Player 1.1.3 - 'wintab32.dll' DLL Hijacking - The Exploit-DB Ref : 14750
Link: http://www.exploit-db.com/exploits/14750

exploitdb
Reference: CVE-2010-3124
Description: VideoLAN VLC Media Player 1.1.3 - 'wintab32.dll' DLL Hijacking
Link: https://www.exploit-db.com/exploits/14750

nvd
Reference: CVE-2010-3124
Description: Untrusted search path vulnerability in bin/winvlc.c in VLC Media Player 1.1.3 and earlier allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse wintab32.dll that is located in the same folder as a .mp3 file.

Link: http://www.exploit-db.com/exploits/14750

seebug
Reference: CVE-2010-3124
Description: VLC Media Player DLL Hijacking Exploit (wintab32.dll)
Link: https://www.seebug.org/vuldb/ssvid-69674

nist-nvd2
Reference: CVE-2010-3124
Description: Untrusted search path vulnerability in bin/winvlc.c in VLC Media Player 1.1.3 and earlier allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse wintab32.dll that is located in the same folder as a .mp3 file.
Link: http://www.exploit-db.com/exploits/14750

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VLC Media Player ActiveX and Plugin Memory Corruption Vulnerabilities

QID:	118671
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/29/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC Media Player is prone to multiple issues caused by memory corruption errors in the ActiveX control and browser Plugin when processing malformed parameters, which could be exploited by attackers to compromise a vulnerable system via a specially crafted Web page.

Affected Versions:
VLC Media Player Version 1.1.4 and prior

IMPACT:

If this vulnerability is successfully exploited, an attacker can execute arbitrary code.

SOLUTION:

There are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKCR\Wow6432Node\CLSID\{9BE31822-FDAD-461B-AD51-BE1D1C159921}\InprocServer32 exists

C:\Program Files (x86)\VideoLAN\VLC\axvlc.dll found
C:\Program Files (x86)\VideoLAN\VLC\axvlc.dll Version is 1.1.1.0

4 VLC Media Player Incorrect Calling Convention Stack Corruption Vulnerability

QID:	118739
Category:	Local
Associated CVEs:	-
Vendor Reference:	VideoLAN-SA-1006
Bugtraq ID:	-
Service Modified:	11/18/2010
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

Due to an error in the declaration of code calling conventions, VLC for Windows suffers from a stack smashing attack in the Samba network share access module.

Affected Versions:
VLC media player versions prior to 1.1.5.

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to execute arbitrary code.

SOLUTION:

The latest patch is available for download fromVLC Web site (http://www.videolan.org/).

Refer to vendor advisory VideoLAN-SA-1006 (http://www.videolan.org/security/sa1004.html) to obtain additional details about the vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1006: Windows (VLC Media Player) (http://sourceforge.net/projects/vlc/files/1.1.5/win32/vlc-1.1.5-win32.exe/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VLC Media Player AMV and NSV Data Processing Memory Corruption Vulnerability

QID:	119092
Category:	Local
Associated CVEs:	CVE-2010-3275, CVE-2010-3276
Vendor Reference:	VLC Media Player
Bugtraq ID:	47012
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC Media Player is prone to a vulnerability that could be exploited by remote attackers to compromise a vulnerable system. This issue is caused by a memory corruption error in the "libdirectx" plugin when processing malformed NSV or AMV data.

Affected Versions:
VLC Media Player Version 1.1.7 and prior.

IMPACT:

If this vulnerability is successfully exploited, a remote attackers can execute arbitrary code by tricking a user into opening a malicious file

or visiting a specially crafted web page.

SOLUTION:

Upgrade to VLC Media Player version 1.1.8. For detailed information and downloading the software, please refer to VLC Media Player 1.1.8 (http://www.videolan.org/vlc/releases/1.1.8.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC Media Player: Windows (http://sourceforge.net/projects/vlc/files/1.1.8/win32/vlc-1.1.8-win32.exe/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2010-3276
Description: VLC Media Player NSV File Memory Corruption Exploit - Core Security Category : Exploits/Client Side

Reference: CVE-2010-3275
Description: VLC Media Player AMV File Memory Corruption Exploit - Core Security Category : Exploits/Client Side

Metasploit

Reference: CVE-2010-3275
Description: VLC AMV Dangling Pointer Vulnerability - Metasploit Ref : /modules/exploit/dialup/multi/login/manyargs
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/vlc_amv.rb

Reference: CVE-2010-3275
Description: VLC AMV Dangling Pointer Vulnerability - Metasploit Ref : /modules/exploit/windows/browser/vlc_amv
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/vlc_amv.rb

The Exploit-DB

Reference: CVE-2010-3275
Description: VideoLAN VLC Media Player 1.1.4 - 'AMV' Dangling Pointer (Metasploit) - The Exploit-DB Ref : 17048
Link: http://www.exploit-db.com/exploits/17048

exploitdb

Reference: CVE-2010-3275
Description: VideoLAN VLC Media Player 1.1.4 - 'AMV' Dangling Pointer (Metasploit)
Link: https://www.exploit-db.com/exploits/17048

nvd

Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.metasploit.com/modules/exploit/windows/browser/vlc_amv

Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.securityfocus.com/bid/47012

Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.exploit-db.com/exploits/17048

Reference: CVE-2010-3276
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an NSV file.
Link: http://www.securityfocus.com/bid/47012

metasploit
Reference: CVE-2010-3275
Description: VLC AMV Dangling Pointer Vulnerability
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2010-3275
Description: VLC AMV Dangling Pointer Vulnerability
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/vlc_amv.rb

coreimpact
Reference: CVE-2010-3275
Description: VLC Media Player AMV File Memory Corruption Exploit
Link: https://www.coresecurity.com/core-labs/exploits

Reference: CVE-2010-3276
Description: VLC Media Player NSV Memory Corruption Exploit
Link: https://www.coresecurity.com/core-labs/exploits

white-phosphorus
Reference: CVE-2010-3275
Description: wp_vlc_mediaplayer_amv
Link: http://exploitlist.immunityinc.com/home/exploitpack/White_Phosphorus/wp_vlc_mediaplayer_amv

nist-nvd2
Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.securityfocus.com/bid/47012

Reference: CVE-2010-3276
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an NSV file.
Link: http://www.securityfocus.com/bid/47012

Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.metasploit.com/modules/exploit/windows/browser/vlc_amv

Reference: CVE-2010-3275
Description: libdirectx_plugin.dll in VideoLAN VLC Media Player before 1.1.8 allows remote attackers to execute arbitrary code via a crafted width in an AMV file, related to a "dangling pointer vulnerability."
Link: http://www.exploit-db.com/exploits/17048

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\plugins\libdirectx_plugin.dll found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VLC Media Player "MP4_ReadBox_skcr()" Buffer Overflow Vulnerability (VideoLAN-SA-1103)

QID:	119143
Category:	Local
Associated CVEs:	CVE-2011-1684
Vendor Reference:	VideoLAN-SA-1103
Bugtraq ID:	47293
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC Media Player is exposed to a buffer overflow vulnerability due to an error within the "MP4_ReadBox_skcr()" function in modules/demux/mp4/libmp4.c. This vulnerability can be exploited to cause a heap-based buffer overflow by tricking a user into opening a specially crafted MP4 file.

Affected Versions:
VLC Media Palyer 1.1.8 and prior

IMPACT:

Successfully exploiting this vulnerability might allow an attacker to execute arbitrary code.

SOLUTION:

Upgrade to VLC Media Player version 1.1.9. For detailed information and downloading the software, please refer to VLC Media Player 1.1.9 (http://www.videolan.org/vlc/releases/1.1.9.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC Media Player (http://sourceforge.net/projects/vlc/files/1.1.8/win32/vlc-1.1.9-win32.exe/download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VLC Media Player MKV Demuxer "MKV_IS_ID" Vulnerability (VideoLAN-SA-1102)

QID:	119236
Category:	Local
Associated CVEs:	CVE-2011-0531
Vendor Reference:	VideoLAN-SA-1102
Bugtraq ID:	46060
Service Modified:	08/15/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

The vulnerability is caused by an input validation error within the "MKV_IS_ID" macro in modules/demux/mkv/mkv.hpp of the MKV demuxer.

Affected Versions:
VLC media player version 1.1.6.1 and prior are affected.

IMPACT:

Successfully exploiting this vulnerability might allow an attacker to execute arbitrary code.

SOLUTION:

Upgrade to VLC Media Player version 1.1.7. For detailed information, please refer to VideoLAN-SA-1102 (http://www.videolan.org/security/sa1102.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

vlc 1.1.7: Windows (http://download.videolan.org/pub/videolan/vlc/1.1.7/win32/vlc-1.1.7-win32.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security
- Reference: CVE-2011-0531
- Description: VLC Media Player MKV File Memory Corruption Exploit - Core Security Category : Exploits/Client Side

Metasploit
- Reference: CVE-2011-0531
- Description: VideoLAN VLC MKV Memory Corruption - Metasploit Ref : /modules/exploit/windows/fileformat/vlc_webm
- Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/fileformat/vlc_webm.rb

- Reference: CVE-2011-0531
- Description: VideoLAN VLC MKV Memory Corruption - Metasploit Ref : /modules/exploit/windows/http/solarwinds_storage_manager_sql
- Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/fileformat/vlc_webm.rb

The Exploit-DB
- Reference: CVE-2011-0531
- Description: VideoLAN VLC Media Player 1.1.6 - 'MKV' Memory Corruption (Metasploit) - The Exploit-DB Ref : 16637
- Link: http://www.exploit-db.com/exploits/16637

exploitdb
- Reference: CVE-2011-0531
- Description: VideoLAN VLC Media Player 1.1.6 - 'MKV' Memory Corruption (Metasploit)
- Link: https://www.exploit-db.com/exploits/16637

seebug
- Reference: CVE-2011-0531
- Description: VideoLAN VLC MKV Memory Corruption
- Link: https://www.seebug.org/vuldb/ssvid-71147

saint
- Reference: CVE-2011-0531
- Description: VideoLAN VLC Media Player MKV Demuxer Code Execution
- Link: https://my.saintcorporation.com/cgi-bin/exploit_info/vlc_mkv_demuxer

packetstorm
- Reference: CVE-2011-0531
- Description: VideoLAN VLC MKV Memory Corruption
- Link: https://packetstormsecurity.com/files/98119/VideoLAN-VLC-MKV-Memory-Corruption.html

metasploit
- Reference: CVE-2011-0531
- Description: VideoLAN VLC MKV Memory Corruption
- Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2011-0531
Description: VideoLAN VLC MKV Memory Corruption
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/fileformat/vlc_webm.rb

coreimpact
Reference: CVE-2011-0531
Description: VLC Media Player MKV File Memory Corruption Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VLC Media Player, RealMedia and AVI File Parsing Vulnerabilities (VideoLAN-SA-1105, VideoLAN-SA-1106)

QID:	119397
Category:	Local
Associated CVEs:	CVE-2011-2587, CVE-2011-2588
Vendor Reference:	VideoLAN-SA-1105, VideoLAN-SA-1106
Bugtraq ID:	48664
Service Modified:	07/14/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC media player is exposed to following vulnerabilities:
1) An integer overflow error when parsing a RealAudio a data block within RealMedia files can be exploited to cause a heap-based buffer overflow.

2) An integer underflow error when parsing the "strf" chunk within AVI files can be exploited to cause a heap-based buffer overflow.

Affected Versions:
VLC Media Player versions prior to 1.1.11

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to execute arbitrary code.

SOLUTION:

Update to Version 1.1.11 to resolve this issue. The latest version is available for download fromVLC Media Player Web site (http://www.videolan.org/vlc/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1105 (http://www.videolan.org/vlc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VideoLAN VLC Media Player Subtitles Remote Code Execution Vulnerability

QID:	370403
Category:	Local
Associated CVEs:	CVE-2017-8310, CVE-2017-8311, CVE-2017-8312, CVE-2017-8313
Vendor Reference:	-
Bugtraq ID:	98638,98634,98631,98633
Service Modified:	08/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project. An unauthenticated remote attacker can upload a specially crafted Subtitles file to the online repository that, when loaded by VLC users, triggers an arbitrary code execution.

Affected Version
VLC Media Player versions prior to 2.2.5

IMPACT:

On successful exploitation it allows remote attackers to execute arbitrary code via a crafted subtitles file.

SOLUTION:

Customers are advised to download the latest version from VLC Media Player Download Page (http://www.videolan.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC 2.2.5.1 (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2017-8311
- Description: VLC Media Player/Kodi/PopcornTime 'Red Chimera' < 2.2.5 - Memory Corruption (PoC) - The Exploit-DB Ref : 44514
- Link: http://www.exploit-db.com/exploits/44514

exploitdb
- Reference: CVE-2017-8311
- Description: VLC Media Player/Kodi/PopcornTime 'Red Chimera' < 2.2.5 - Memory Corruption (PoC)
- Link: https://www.exploit-db.com/exploits/44514

packetstorm
- Reference: CVE-2017-8311
- Description: VLC Media Player/Kodi/PopcornTime Memory Corruption
- Link: https://packetstormsecurity.com/files/147335/VLC-Media-Player-Kodi-PopcornTime-Memory-Corruption.html

0day.today

Reference: CVE-2017-8311
Description: VLC Media Player/Kodi/PopcornTime Red Chimera < 2.2.5 - Memory Corruption Exploit (PoC)
Link: https://0day.today/exploit/29940

nist-nvd2
Reference: CVE-2017-8311
Description: Potential heap based buffer overflow in ParseJSS in VideoLAN VLC before 2.2.5 due to skipping NULL terminator in an input string allows attackers to execute arbitrary code via a crafted subtitles file.
Link: https://www.exploit-db.com/exploits/44514/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VideoLAN VLC media player Remote Code Execution Vulnerability

QID:	372023
Category:	Local
Associated CVEs:	CVE-2019-13615
Vendor Reference:	VideLAN VLC Media Player
Bugtraq ID:	109304
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

VideoLAN VLC media player has a heap-based buffer over-read in mkv::demux_sys_t::FreeUnused() in modules/demux/mkv/demux.cpp when called from mkv::Open in modules/demux/mkv/mkv.cpp.

An attacker can exploit this vulnerability by sending a crafted multimedia file targeting the vulnerable machine. Until VLC released fixes it is recommended not to download and run multimedia files from untrusted sources.

Affected Version:VideoLAN VLC media player prior to 3.0.3

IMPACT:

A remote attacker can exploit this vulnerability to run arbitrary code on the target machine which causes a denial of service state, disclose information, or manipulate files.

SOLUTION:

The Vendor has released patch. Please download the latest version of VLC Media Player (https://www.videolan.org/vlc/index.html).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC Media Player (https://www.videolan.org/vlc/index.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd
Reference: CVE-2019-13615
Description: libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextElement.

Link: https://trac.videolan.org/vlc/ticket/22474

nist-nvd2

Reference: CVE-2019-13615

Description: libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextElement.

Link: https://trac.videolan.org/vlc/ticket/22474

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VideoLAN VLC Media player Multiple Vulnerabilities (VideoLAN-SB-VLC-3013)

QID:	375560
Category:	Local
Associated CVEs:	-
Vendor Reference:	VideoLAN-SB-VLC-3013
Bugtraq ID:	-
Service Modified:	05/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:
VLC media player 3.0.12 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has confirmed the vulnerability and released VLC media player version 3.0.13 to resolve this issue. Download the latest verison of vlc from here (https://www.videolan.org/vlc/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3013 (http://www.videolan.org/security/sb-vlc3013.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 VideoLAN VLC Media player Multiple Vulnerabilities (VideoLAN-SB-VLC-3012)

QID:	376463
Category:	Local
Associated CVEs:	-
Vendor Reference:	VideoLAN-SB-VLC-3012
Bugtraq ID:	-
Service Modified:	03/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:VLC media player 3.0.11 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to VideoLAN-SB-VLC-3012 (https://www.videolan.org/security/sb-vlc3012.html) to obtain more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3012 (https://www.videolan.org/security/sb-vlc3012.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-40)

QID:	377600
Category:	Local
Associated CVEs:	CVE-2022-40956, CVE-2022-40962, CVE-2022-40960, CVE-2022-40959, CVE-2022-40957, CVE-2022-40958, CVE-2022-40961
Vendor Reference:	MFSA2022-40
Bugtraq ID:	-
Service Modified:	01/04/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2022-40959: Bypassing FeaturePolicy restrictions on transient pages

CVE-2022-40960: Data-race when parsing non-UTF-8 URLs in threads
CVE-2022-40958: Bypassing Secure Context restriction for cookies with __Host and __Secure prefix
CVE-2022-40961: Stack-buffer overflow when initializing Graphics
CVE-2022-40956: Content-Security-Policy base-uri bypass
CVE-2022-40957: Incoherent instruction cache when building WASM on ARM64
CVE-2022-40962: Memory safety bugs fixed in Firefox 105 and Firefox ESR 102.3

Affected Products:
Prior to Firefox 105

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2022-40 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-40/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2022-40 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-40/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-44)

QID:	377641
Category:	Local
Associated CVEs:	CVE-2022-42929, CVE-2022-42927, CVE-2022-42928, CVE-2022-42930, CVE-2022-42931, CVE-2022-42932, CVE-2022-46881, CVE-2022-46885
Vendor Reference:	MFSA2022-44
Bugtraq ID:	-
Service Modified:	02/07/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2022-42927: Same-origin policy violation could have leaked cross-origin URLs
CVE-2022-42928: Memory Corruption in JS Engine
CVE-2022-42929: Denial of Service via window.print
CVE-2022-42930: Race condition in DOM Workers
CVE-2022-42931: Username saved to a plaintext file on disk
CVE-2022-42932: Memory safety bugs fixed in Firefox 106 and Firefox ESR 102.4

Affected Products:
Prior to Firefox 106

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2022-44 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-44/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2022-44 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-44/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 VideoLAN VLC Media player Multiple Vulnerabilities (VideoLAN-SB-VLC-3018)

QID:	377802
Category:	Local
Associated CVEs:	CVE-2022-41325
Vendor Reference:	VideoLAN-SB-VLC-3018
Bugtraq ID:	-
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:VLC media player 3.0.17 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to VideoLAN-SB-VLC-3018 (https://www.videolan.org/security/sb-vlc3018.html) to obtain more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3018 (https://www.videolan.org/security/sb-vlc3018.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference:	CVE-2022-41325
Description:	An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.17.4 allows attackers, by tricking a user into opening a crafted playlist or connecting to a rogue VNC server, to crash VLC or execute code under some conditions.
Link:	https://www.synacktiv.com/sites/default/files/2022-11/vlc_vnc_int_overflow-CVE-2022-41325.pdf

nist-nvd2

Reference: CVE-2022-41325

Description: An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.17.4 allows attackers, by tricking a user into opening a crafted playlist or connecting to a rogue VNC server, to crash VLC or execute code under some conditions.

Link: https://www.synacktiv.com/sites/default/files/2022-11/vlc_vnc_int_overflow-CVE-2022-41325.pdf

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-51)

QID:	377829
Category:	Local
Associated CVEs:	CVE-2022-46877, CVE-2022-46873, CVE-2022-46874, CVE-2022-46871, CVE-2022-46879, CVE-2022-46878, CVE-2022-46872, CVE-2022-46875
Vendor Reference:	MFSA2022-51
Bugtraq ID:	-
Service Modified:	01/05/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2022-46871: libusrsctp library out of date
CVE-2022-46872: Arbitrary file read from a compromised content process
CVE-2022-46873: Firefox did not implement the CSP directive unsafe-hashes
CVE-2022-46874: Drag and Dropped Filenames could have been truncated to malicious extensions
CVE-2022-46875: Download Protections were bypassed by .atloc and .ftploc files on Mac OS
CVE-2022-46877: Fullscreen notification bypass
CVE-2022-46878: Memory safety bugs fixed in Firefox 108 and Firefox ESR 102.6
CVE-2022-46879: Memory safety bugs fixed in Firefox 108

Affected Products:
Prior to Firefox 108

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2022-51 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2022-51 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-01)

QID:	377905
Category:	Local
Associated CVEs:	CVE-2023-23605, CVE-2023-23601, CVE-2023-23604, CVE-2023-23606, CVE-2023-23597, CVE-2023-23600, CVE-2023-23599, CVE-2023-23598, CVE-2023-23602, CVE-2023-23603
Vendor Reference:	MFSA2023-01
Bugtraq ID:	-
Service Modified:	06/09/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-23597: Logic bug in process allocation allowed to read arbitrary files
CVE-2023-23598: Arbitrary file read from GTK drag and drop on Linux
CVE-2023-23599: Malicious command could be hidden in devtools output on Windows
CVE-2023-23600: Notification permissions persisted between Normal and Private Browsing on Android
CVE-2023-23601: URL being dragged from cross-origin iframe into same tab triggers navigation
CVE-2023-23602: Content Security Policy wasn't being correctly applied to WebSockets in WebWorkers
CVE-2023-23603: Calls to console.log allowed bypasing Content Security Policy via format directive
CVE-2023-23604: Creation of duplicate SystemPrincipal from less secure contexts
CVE-2023-23605: Memory safety bugs fixed in Firefox 109 and Firefox ESR 102.7
CVE-2023-23606: Memory safety bugs fixed in Firefox 109

Affected Products:
Prior to Firefox 109

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2023-01 or later
(https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-05)

QID:	377975
Category:	Local
Associated CVEs:	CVE-2023-25729, CVE-2023-25734, CVE-2023-25740, CVE-2023-25736, CVE-2023-25732, CVE-2023-25735, CVE-2023-0767, CVE-2023-25738, CVE-2023-25743, CVE-2023-25737, CVE-2023-25742, CVE-2023-25745, CVE-2023-25730, CVE-2023-25733, CVE-2023-25741, CVE-2023-25739, CVE-2023-25731, CVE-2023-25728, CVE-2023-25744
Vendor Reference:	MFSA2023-05
Bugtraq ID:	-
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-25728: Content security policy leak in violation reports using iframes
CVE-2023-25730: Screen hijack via browser fullscreen mode
CVE-2023-25743: Fullscreen notification not shown in Firefox Focus
CVE-2023-0767: Arbitrary memory write via PKCS 12 in NSS
CVE-2023-25735: Potential use-after-free from compartment mismatch in SpiderMonkey
CVE-2023-25737: Invalid downcast in SVGUtils::SetupStrokeGeometry
CVE-2023-25738: Printing on Windows could potentially crash Firefox with some device drivers
CVE-2023-25739: Use-after-free in mozilla::dom::ScriptLoadContext::~ScriptLoadContext
CVE-2023-25729: Extensions could have opened external schemes without user knowledge
CVE-2023-25732: Out of bounds memory write from EncodeInputStream
CVE-2023-25734: Opening local .url files could cause unexpected network loads
CVE-2023-25740: Opening local .scf files could cause unexpected network loads
CVE-2023-25731: Prototype pollution when rendering URLPreview
CVE-2023-25733: Possible null pointer dereference in TaskbarPreviewCallback
CVE-2023-25736: Invalid downcast in GetTableSelectionMode
CVE-2023-25741: Same-origin policy leak via image drag and drop
CVE-2023-25742: Web Crypto ImportKey crashes tab
CVE-2023-25744: Memory safety bugs fixed in Firefox 110 and Firefox ESR 102.8
CVE-2023-25745: Memory safety bugs fixed in Firefox 110

Affected Products:
Prior to Firefox 110

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2023-05 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference:	CVE-2023-25734
Description:	After downloading a Windows .url shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource.*This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8.
Link:	https://bugzilla.mozilla.org/show_bug.cgi?id=1784451
Reference:	CVE-2023-25741
Description:	When dragging and dropping an image cross-origin, the image's size could potentially be leaked. This behavior was shipped in

109 and caused web compatibility problems as well as this security concern, so the behavior was disabled until further review. This vulnerability affects Firefox < 110.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1812611

nist-nvd2

Reference: CVE-2023-25734

Description: After downloading a Windows .url shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource.*This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1784451

Reference: CVE-2023-25741

Description: When dragging and dropping an image cross-origin, the image's size could potentially be leaked. This behavior was shipped in 109 and caused web compatibility problems as well as this security concern, so the behavior was disabled until further review. This vulnerability affects Firefox < 110.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1812611

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-09)

QID:	378072
Category:	Local
Associated CVEs:	CVE-2023-25750, CVE-2023-28162, CVE-2023-25749, CVE-2023-28164, CVE-2023-25751, CVE-2023-28159, CVE-2023-28176, CVE-2023-28160, CVE-2023-28161, CVE-2023-25748, CVE-2023-25752, CVE-2023-28177, CVE-2023-28163
Vendor Reference:	MFSA2023-09
Bugtraq ID:	-
Service Modified:	06/29/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-28159: Fullscreen Notification could have been hidden by download popups on Android
CVE-2023-25748: Fullscreen Notification could have been hidden by window prompts on Android
CVE-2023-25749: Firefox for Android may have opened third-party apps without a prompt
CVE-2023-25750: Potential ServiceWorker cache leak during private browsing mode
CVE-2023-25751: Incorrect code generation during JIT compilation
CVE-2023-28160: Redirect to Web Extension files may have leaked local path
CVE-2023-28164: URL being dragged from a removed cross-origin iframe into the same tab triggered navigation
CVE-2023-28161: One-time permissions granted to a local file were extended to other local files loaded in the same tab
CVE-2023-28162: Invalid downcast in Worklets
CVE-2023-25752: Potential out-of-bounds when accessing throttled streams
CVE-2023-28163: Windows Save As dialog resolved environment variables
CVE-2023-28176: Memory safety bugs fixed in Firefox 111 and Firefox ESR 102.9
CVE-2023-28177: Memory safety bugs fixed in Firefox 111

Affected Products:
Prior to Firefox 111

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities.Upgrading to Firefox 111 will fix the vulnerability, for more information you can refer MFSA2023-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Microsoft WinVerifyTrust Signature Validation Vulnerability

QID:	378332
Category:	Local
Associated CVEs:	CVE-2013-3900
Vendor Reference:	CVE-2013-3900
Bugtraq ID:	-
Service Modified:	09/13/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft stated that they have re-published the CVE-2013-3900 to inform customers about the availability of EnableCertPaddingCheck. This behavior remains available as an opt-in feature via the registry key setting and is available on all supported editions of Windows released since December 10, 2013.

Microsoft recommends that executable authors consider conforming all signed binaries to the new verification standard by ensuring that they contain no extraneous information in the WIN_CERTIFICATE structure. Microsoft also recommends that customers appropriately test this change to evaluate how it will behave in their environments.

Microsoft recommends that customers test how this change to Authenticode signature verification behaves in their environment before fully implementing it. To enable the Authenticode signature verification improvements, modify the registry to add the EnableCertPaddingCheck value as detailed below.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"

IMPACT:

A remote code execution vulnerability exists in the way that the WinVerifyTrust function handles Windows Authenticode signature verification for portable executable (PE) files. An anonymous attacker could exploit the vulnerability by modifying an existing signed executable file to leverage unverified portions of the file in such a way as to add malicious code to the file without invalidating the signature.

SOLUTION:

Customers are advised to refer to WinVerifyTrust Signature Validation (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900) for further details pertaining to this.

Opting into this stricter verification behavior causes the WinVerifyTrust function to perform strict Windows Authenticode signature verification for PE files. After opting-in, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification. This may impact some installers. If you are using an installer that is impacted, Microsoft recommends using an installer that only extracts content from validated portions of the signed file.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2013-3900
Description:	med0x2e/SigFlip exploit repository
Link:	https://github.com/med0x2e/SigFlip

cisa-kev

Reference:	CVE-2013-3900
Description:	Microsoft WinVerifyTrust function Remote Code Execution
Link:	https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

microsoft-cvrf

Reference:	CVE-2013-3900
Description:	WinVerifyTrust Signature Validation Vulnerability
Link:	https://api.msrc.microsoft.com/cvrf/2022-Jan?api-version=2020

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	Generic
Type:	Rootkit
Platform:	Win64

Malware ID:	CVE-2013-3900
Type:	Exploit
Platform:	Win64,Win32

Qualys Cloud Threat DB

Malware ID:	Conti
Type:	Ransomware
Link:	https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html

RESULTS:

HKLM\Software\Microsoft\Cryptography\Wintrust\Config EnableCertPaddingCheck is missing.
HKLM\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config EnableCertPaddingCheck is missing.

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-13)

QID:	378383
Category:	Local
Associated CVEs:	CVE-2023-29545, CVE-2023-29540, CVE-2023-29533, CVE-2023-29531, CVE-2023-28163, CVE-2023-29532, CVE-2023-29549, CVE-2023-29538, CVE-2023-29551, CVE-2023-29534, CVE-2023-29544, CVE-2023-29536, CVE-2023-29537, CVE-2023-29541, CVE-2023-29548, CVE-2023-29546, CVE-2023-29543, CVE-2023-29542, CVE-2023-29550, CVE-2023-29539, CVE-2023-29547, CVE-2023-29535
Vendor Reference:	MFSA2023-13
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-29531: Out-of-bound memory access in WebGL on macOS
CVE-2023-29532: Mozilla Maintenance Service Write-lock bypass
CVE-2023-29533: Fullscreen notification obscured
CVE-2023-29534: Fullscreen notification could have been obscured on Firefox for Android
CVE-2023-29535: Potential Memory Corruption following Garbage Collector compaction
CVE-2023-29536: Invalid free from JavaScript code
CVE-2023-29537: Data Races in font initialization code
CVE-2023-29538: Directory information could have been leaked to WebExtensions
CVE-2023-29539: Content-Disposition filename truncation leads to Reflected File Download
CVE-2023-29540: Iframe sandbox bypass using redirects and sourceMappingUrls
CVE-2023-29541: Files with malicious extensions could have been downloaded unsafely on Linux
CVE-2023-29542: Bypass of file download extension restrictions
CVE-2023-29543: Use-after-free in debugging APIs
CVE-2023-29544: Memory Corruption in garbage collector
CVE-2023-29545: Windows Save As dialog resolved environment variables
CVE-2023-29546: Screen recording in Private Browsing included address bar on Android
CVE-2023-29547: Secure document cookie could be spoofed with insecure cookie
CVE-2023-29548: Incorrect optimization result on ARM64
CVE-2023-29549: Javascript's bind function may have failed
CVE-2023-29550: Memory safety bugs fixed in Firefox 112 and Firefox ESR 102.10
CVE-2023-29551: Memory safety bugs fixed in Firefox 112

Affected Products:
Prior to Firefox 112

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2023-13 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-13 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-16)

QID:	378475
Category:	Local
Associated CVEs:	CVE-2023-32211, CVE-2023-32208, CVE-2023-32214, CVE-2023-32216, CVE-2023-32212, CVE-2023-32207, CVE-2023-32205, CVE-2023-32206, CVE-2023-32215, CVE-2023-32213, CVE-2023-32209, CVE-2023-32210
Vendor Reference:	MFSA2023-16
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-32205: Browser prompts could have been obscured by popups
CVE-2023-32206: Crash in RLBox Expat driver
CVE-2023-32207: Potential permissions request bypass via clickjacking
CVE-2023-32208: Leak of script base URL in service workers via import()
CVE-2023-32209: Persistent DoS via favicon image
CVE-2023-32210: Incorrect principal object ordering
CVE-2023-32211: Content process crash due to invalid wasm code
CVE-2023-32212: Potential spoof due to obscured address bar
CVE-2023-32213: Potential memory corruption in FileReader::DoReadData()
CVE-2023-32214: Potential DoS via exposed protocol handlers
CVE-2023-32215: Memory safety bugs fixed in Firefox 113 and Firefox ESR 102.11
CVE-2023-32216: Memory safety bugs fixed in Firefox 113

Affected Products:
Prior to Firefox 113

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2023-16 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-16/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-16 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-16/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-20)

QID:	378556
Category:	Local
Associated CVEs:	CVE-2023-34414, CVE-2023-34415, CVE-2023-34417, CVE-2023-34416
Vendor Reference:	MFSA2023-20
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to

CVE-2023-34414: Click-jacking certificate exceptions through rendering lag
CVE-2023-34415: Site-isolation bypass on sites that allow open redirects to data: urls
CVE-2023-34416: Memory safety bugs fixed in Firefox 114 and Firefox ESR 102.12
CVE-2023-34417: Memory safety bugs fixed in Firefox 114

Affected Products:
Prior to Firefox 114

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2023-20 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-20/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-20/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-22)

QID:	378630
Category:	Local
Associated CVEs:	CVE-2023-37207, CVE-2023-37202, CVE-2023-37204, CVE-2023-37210, CVE-2023-37205, CVE-2023-37201, CVE-2023-37203, CVE-2023-37206, CVE-2023-37208, CVE-2023-37209, CVE-2023-37211, CVE-2023-37212, CVE-2023-3482
Vendor Reference:	MFSA2023-22
Bugtraq ID:	-
Service Modified:	07/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-3482: Block all cookies bypass for localstorage
CVE-2023-37201: Use-after-free in WebRTC certificate generation
CVE-2023-37202: Potential use-after-free from compartment mismatch in SpiderMonkey
CVE-2023-37203: Drag and Drop API may provide access to local system files
CVE-2023-37204: Fullscreen notification obscured via option element
CVE-2023-37205: URL spoofing in address bar using RTL characters
CVE-2023-37206: Insufficient validation of symlinks in the FileSystem API
CVE-2023-37207: Fullscreen notification obscured
CVE-2023-37208: Lack of warning when opening Diagcab files
CVE-2023-37209: Use-after-free in `NotifyOnHistoryReload`
CVE-2023-37210: Full-screen mode exit prevention
CVE-2023-37211: Memory safety bugs fixed in Firefox 115, Firefox ESR 102.13, and Thunderbird 102.13
CVE-2023-37212: Memory safety bugs fixed in Firefox 115

Affected Products:
Prior to Firefox 115

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 115 to fix vulnerability, you can also refer MFSA2023-22 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-22/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-22 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-22/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference:	CVE-2023-37206
Description:	Uploading files which contain symlinks may have allowed an attacker to trick a user into submitting sensitive data to a malicious website. This vulnerability affects Firefox < 115.
Link:	https://bugzilla.mozilla.org/show_bug.cgi?id=1813299

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-26)

QID:	378656
Category:	Local
Associated CVEs:	CVE-2023-3600
Vendor Reference:	MFSA2023-26
Bugtraq ID:	-
Service Modified:	07/21/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-3600: Use-after-free in workers

Affected Products:
Prior to Firefox 115.0.2

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 115.0.2 to fix vulnerability, you can also refer MFSA2023-26 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-26/) for more details.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-26 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-26/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-29)

QID:	378726
Category:	Local
Associated CVEs:	CVE-2023-4056, CVE-2023-4053, CVE-2023-4055, CVE-2023-4052, CVE-2023-4057, CVE-2023-4058, CVE-2023-4049, CVE-2023-4047, CVE-2023-4050, CVE-2023-4045, CVE-2023-4046, CVE-2023-4048, CVE-2023-4051, CVE-2023-4054
Vendor Reference:	MFSA2023-29
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-4045: Offscreen Canvas could have bypassed cross-origin restrictions
CVE-2023-4046: Incorrect value used during WASM compilation
CVE-2023-4047: Potential permissions request bypass via clickjacking
CVE-2023-4048: Crash in DOMParser due to out-of-memory conditions
CVE-2023-4049: Fix potential race conditions when releasing platform objects
CVE-2023-4050: Stack buffer overflow in StorageManager
CVE-2023-4051: Full screen notification obscured by file open dialog
CVE-2023-4052: File deletion and privilege escalation through Firefox uninstaller
CVE-2023-4053: Full screen notification obscured by external program
CVE-2023-4054: Lack of warning when opening appref-ms files
CVE-2023-4055: Cookie jar overflow caused unexpected cookie jar state
CVE-2023-4056: Memory safety bugs fixed in Firefox 116, Firefox ESR 115.1, Firefox ESR 102.14, Thunderbird 115.1, and Thunderbird 102.14
CVE-2023-4057: Memory safety bugs fixed in Firefox 116, Firefox ESR 115.1, and Thunderbird 115.1
CVE-2023-4058: Memory safety bugs fixed in Firefox 116

Affected Products:
Prior to Firefox 116

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 116 to fix vulnerability, you can also refer MFSA2023-29 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-29 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-34)

QID:	378816
Category:	Local
Associated CVEs:	CVE-2023-4576, CVE-2023-4584, CVE-2023-4577, CVE-2023-4574, CVE-2023-4578, CVE-2023-4582, CVE-2023-4573, CVE-2023-4580, CVE-2023-4575, CVE-2023-4581, CVE-2023-4583, CVE-2023-4579, CVE-2023-4585
Vendor Reference:	MFSA2023-34
Bugtraq ID:	-
Service Modified:	09/14/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-4573: Memory corruption in IPC CanvasTranslator
CVE-2023-4574: Memory corruption in IPC ColorPickerShownCallback
CVE-2023-4575: Memory corruption in IPC FilePickerShownCallback
CVE-2023-4576: Integer Overflow in RecordedSourceSurfaceCreation
CVE-2023-4577: Memory corruption in JIT UpdateRegExpStatics
CVE-2023-4578: Error reporting methods in SpiderMonkey could have triggered an Out of Memory Exception
CVE-2023-4579: Persisted search terms were formatted as URLs
CVE-2023-4580: Push notifications saved to disk unencrypted
CVE-2023-4581: XLL file extensions were downloadable without warnings
CVE-2023-4582: Buffer Overflow in WebGL glGetProgramiv
CVE-2023-4583: Browsing Context potentially not cleared when closing Private Window
CVE-2023-4584: Memory safety bugs fixed in Firefox 117, Firefox ESR 102.15, Firefox ESR 115.2, Thunderbird 102.15, and Thunderbird 115.2
CVE-2023-4585: Memory safety bugs fixed in Firefox 117, Firefox ESR 115.2, and Thunderbird 115.2

Affected Products:
Prior to Firefox 117

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 117 to fix vulnerability, you can also refer MFSA2023-34 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-34/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-34 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-34/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-41)

QID:	378900
Category:	Local
Associated CVEs:	CVE-2023-5173, CVE-2023-5168, CVE-2023-5171, CVE-2023-5169, CVE-2023-5175, CVE-2023-5172, CVE-2023-5174, CVE-2023-5170, CVE-2023-5176
Vendor Reference:	MFSA2023-41
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-5168: Out-of-bounds write in FilterNodeD2D1
CVE-2023-5169: Out-of-bounds write in PathOps
CVE-2023-5170: Memory leak from a privileged process
CVE-2023-5171: Use-after-free in Ion Compiler
CVE-2023-5172: Memory Corruption in Ion Hints
CVE-2023-5173: Out-of-bounds write in HTTP Alternate Services
CVE-2023-5174: Double-free in process spawning on Windows
CVE-2023-5175: Use-after-free of ImageBitmap during process shutdown
CVE-2023-5176: Memory safety bugs fixed in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3

Affected Products:
Prior to Firefox 118

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 118 to fix vulnerability, you can also refer MFSA2023-41 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-41/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-41 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-41/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-44)

QID:	378906
Category:	Local
Associated CVEs:	CVE-2023-5217
Vendor Reference:	MFSA2023-44
Bugtraq ID:	-
Service Modified:	03/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-5217: Heap buffer overflow in libvpx

Affected Products:
Prior to Firefox 118.0.1

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 118.0.1 to fix vulnerability, you can also refer MFSA2023-44 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-44 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2023-5217
Description:	wrv/cve-2023-5217-poc exploit repository
Link:	https://github.com/wrv/cve-2023-5217-poc
Reference:	CVE-2023-5217
Description:	UT-Security/cve-2023-5217-poc exploit repository
Link:	https://github.com/UT-Security/cve-2023-5217-poc

cisa-kev

Reference:	CVE-2023-5217
Description:	Google Chrome libvpx Heap Buffer Overflow Vulnerability
Link:	https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference:	CVE-2023-5217
Description:	Google Chrome Heap buffer overflow in vp8 encoding in libvpx
Link:	https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

microsoft-cvrf

Reference:	CVE-2023-5217
Description:	Chromium: CVE-2023-5217 Heap buffer overflow in vp8 encoding in libvpx
Link:	https://api.msrc.microsoft.com/cvrf/2023-Sep?api-version=2020

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-45)

QID:	378958
Category:	Local
Associated CVEs:	CVE-2023-5726, CVE-2023-5722, CVE-2023-5730, CVE-2023-5725, CVE-2023-5724, CVE-2023-5723, CVE-2023-5727, CVE-2023-5729, CVE-2023-5728, CVE-2023-5731, CVE-2023-5721
Vendor Reference:	MFSA2023-45
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-5721: Queued up rendering could have allowed websites to clickjack
CVE-2023-5722: Cross-Origin size and header leakage
CVE-2023-5723: Invalid cookie characters could have led to unexpected errors
CVE-2023-5724: Large WebGL draw could have led to a crash
CVE-2023-5725: WebExtensions could open arbitrary URLs
CVE-2023-5726: Full screen notification obscured by file open dialog on macOS
CVE-2023-5727: Download Protections were bypassed by .msix, .msixbundle, .appx, and .appxbundle files on Windows
CVE-2023-5728: Improper object tracking during GC in the JavaScript engine could have led to a crash.
CVE-2023-5729: Fullscreen notification dialog could have been obscured by WebAuthn prompts
CVE-2023-5730: Memory safety bugs fixed in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4
CVE-2023-5731: Memory safety bugs fixed in Firefox 119

Affected Products:
Prior to Firefox 119

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 119 to fix vulnerability, you can also refer MFSA2023-45 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-45 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-49)

QID:	379062
Category:	Local
Associated CVEs:	CVE-2023-6204, CVE-2023-6205, CVE-2023-6206, CVE-2023-6207, CVE-2023-6208, CVE-2023-6209, CVE-2023-6210, CVE-2023-6211, CVE-2023-6212, CVE-2023-6213
Vendor Reference:	MFSA2023-49
Bugtraq ID:	-
Service Modified:	12/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed by the Mozilla Foundation and its subsidiary for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-6204: Out-of-bound memory access in WebGL2 blitFramebuffer
CVE-2023-6205: Use-after-free in MessagePort::Entangled
CVE-2023-6206: Clickjacking permission prompts using the fullscreen transition
CVE-2023-6207: Use-after-free in ReadableByteStreamQueueEntry::Buffer
CVE-2023-6208: Using Selection API would copy contents into X11 primary selection.
CVE-2023-6209: Incorrect parsing of relative URLs starting with "///"
CVE-2023-6210: Mixed-content resources not blocked in a javascript: pop-up
CVE-2023-6211: Clickjacking to load insecure pages in HTTPS-only mode
CVE-2023-6212: Memory safety bugs fixed in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5
CVE-2023-6213: Memory safety bugs fixed in Firefox 120

Affected Products:
Prior to Firefox 120

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach like evidence of memory corruption or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 120 to fix vulnerability, you can also refer MFSA2023-49 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-49/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-49 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-49/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-56)

QID:	379170
Category:	Local

Associated CVEs:	CVE-2023-6857, CVE-2023-6858, CVE-2023-6871, CVE-2023-6856, CVE-2023-6868, CVE-2023-6872, CVE-2023-6866, CVE-2023-6867, CVE-2023-6873, CVE-2023-6869, CVE-2023-6135, CVE-2023-6859, CVE-2023-6865, CVE-2023-6860, CVE-2023-6863, CVE-2023-6864, CVE-2023-6870, CVE-2023-6861
Vendor Reference:	MFSA2023-56
Bugtraq ID:	-
Service Modified:	12/23/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2023-6856: Heap-buffer-overflow affecting WebGL DrawElementsInstanced method with Mesa VM driver
CVE-2023-6135: NSS susceptible to "Minerva" attack
CVE-2023-6865: Potential exposure of uninitialized data in EncryptingOutputStream
CVE-2023-6857: Symlinks may resolve to smaller than expected buffers
CVE-2023-6858: Heap buffer overflow in nsTextFragment
CVE-2023-6859: Use-after-free in PR_GetIdentitiesLayer
CVE-2023-6866: TypedArrays lack sufficient exception handling
CVE-2023-6860: Potential sandbox escape due to VideoBridge lack of texture validation
CVE-2023-6867: Clickjacking permission prompts using the popup transition
CVE-2023-6861: Heap buffer overflow affected nsWindow::PickerOpen(void) in headless mode
CVE-2023-6868: WebPush requests on Firefox for Android did not require VAPID key
CVE-2023-6869: Content can paint outside of sandboxed iframe
CVE-2023-6870: Android Toast notifications may obscure fullscreen event notifications
CVE-2023-6871: Lack of protocol handler warning in some instances
CVE-2023-6872: Browsing history leaked to syslogs via GNOME
CVE-2023-6863: Undefined behavior in ShutdownObserver()
CVE-2023-6864: Memory safety bugs fixed in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6
CVE-2023-6873: Memory safety bugs fixed in Firefox 121

Affected Products:
Prior to Firefox 121

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 121 to fix vulnerability, you can also refer MFSA2023-56 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-56/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-56 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-56/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference:	CVE-2023-6872
Description:	Browser tab titles were being leaked by GNOME to system logs. This could potentially expose the browsing habits of users running in a private tab. This vulnerability affects Firefox < 121.
Link:	https://bugzilla.mozilla.org/show_bug.cgi?id=1849186

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-01)

QID:	379315
Category:	Local
Associated CVEs:	CVE-2024-0753, CVE-2024-0742, CVE-2024-0749, CVE-2024-0744, CVE-2024-0748, CVE-2024-0741, CVE-2024-0745, CVE-2024-0750, CVE-2024-0754, CVE-2024-0755, CVE-2024-0751, CVE-2024-0743, CVE-2024-0746, CVE-2024-0752, CVE-2024-0747
Vendor Reference:	MFSA2024-01
Bugtraq ID:	-
Service Modified:	08/15/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-0741: Out of bounds write in ANGLE
CVE-2024-0742: Failure to update user input timestamp
CVE-2024-0743: Crash in NSS TLS method
CVE-2024-0744: Wild pointer dereference in JavaScript
CVE-2024-0745: Stack buffer overflow in WebAudio
CVE-2024-0746: Crash when listing printers on Linux
CVE-2024-0747: Bypass of Content Security Policy when directive unsafe-inline was set
CVE-2024-0748: Compromised content process could modify document URI
CVE-2024-0749: Phishing site popup could show local origin in address bar
CVE-2024-0750: Potential permissions request bypass via clickjacking
CVE-2024-0751: Privilege escalation through devtools
CVE-2024-0752: Use-after-free could occur when applying update on macOS
CVE-2024-0753: HSTS policy on subdomain could bypass policy of upper domain
CVE-2024-0754: Crash when using some WASM files in devtools
CVE-2024-0755: Memory safety bugs fixed in Firefox 122, Firefox ESR 115.7, and Thunderbird 115.7

Affected Products:
Prior to Firefox 122

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 122 to fix vulnerability, you can also refer MFSA2024-01 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-01/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-01/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2024-0741
Description:	HyHy100/Firefox-ANGLE-CVE-2024-0741 exploit repository
Link:	https://github.com/HyHy100/Firefox-ANGLE-CVE-2024-0741

Reference:	CVE-2024-0741
Description:	HyHy100/Firefox-CVE-2024-0741 exploit repository
Link:	https://github.com/HyHy100/Firefox-CVE-2024-0741

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-05)

QID:	379392
Category:	Local
Associated CVEs:	CVE-2024-1551, CVE-2024-1548, CVE-2024-1555, CVE-2024-1556, CVE-2024-1547, CVE-2024-1546, CVE-2024-1549, CVE-2024-1557, CVE-2024-1550, CVE-2024-1554, CVE-2024-1553, CVE-2024-1552
Vendor Reference:	MFSA2024-05
Bugtraq ID:	-
Service Modified:	08/22/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-1546: Out-of-bounds memory read in networking channels
CVE-2024-1547: Alert dialog could have been spoofed on another site
CVE-2024-1554: fetch could be used to effect cache poisoning
CVE-2024-1548: Fullscreen Notification could have been hidden by select element
CVE-2024-1549: Custom cursor could obscure the permission dialog
CVE-2024-1550: Mouse cursor re-positioned unexpectedly could have led to unintended permission grants
CVE-2024-1551: Multipart HTTP Responses would accept the Set-Cookie header in response parts
CVE-2024-1555: SameSite cookies were not properly respected when opening a website from an external browser
CVE-2024-1556: Invalid memory access in the built-in profiler
CVE-2024-1552: Incorrect code generation on 32-bit ARM devices
CVE-2024-1553: Memory safety bugs fixed in Firefox 123, Firefox ESR 115.8, and Thunderbird 115.8
CVE-2024-1557: Memory safety bugs fixed in Firefox 123

Affected Products:
Prior to Firefox 123

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 123 to fix vulnerability, you can also refer MFSA2024-05 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-05/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-05/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-12)

QID:	379518
Category:	Local
Associated CVEs:	CVE-2024-2606, CVE-2024-2611, CVE-2024-2610, CVE-2024-2608, CVE-2023-5388, CVE-2024-2615, CVE-2024-2612, CVE-2024-2607, CVE-2024-2609, CVE-2024-2614, CVE-2024-2605, CVE-2024-2613
Vendor Reference:	MFSA2024-12
Bugtraq ID:	-
Service Modified:	08/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-2605: Windows Error Reporter could be used as a Sandbox escape vector
CVE-2024-2606: Mishandling of WASM register values
CVE-2024-2607: JIT code failed to save return registers on Armv7-A
CVE-2024-2608: Integer overflow could have led to out of bounds write
CVE-2023-5388: NSS susceptible to timing attack against RSA decryption
CVE-2024-2609: Permission prompt input delay could expire when not in focus
CVE-2024-2610: Improper handling of html and body tags enabled CSP nonce leakage
CVE-2024-2611: Clickjacking vulnerability could have led to a user accidentally granting permissions
CVE-2024-2612: Self referencing object could have potentially led to a use-after-free
CVE-2024-2613: Improper handling of QUIC ACK frame data could have led to OOM
CVE-2024-2614: Memory safety bugs fixed in Firefox 124, Firefox ESR 115.9, and Thunderbird 115.9
CVE-2024-2615: Memory safety bugs fixed in Firefox 124

Affected Products:
Prior to Firefox 124

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 124 to fix vulnerability, you can also refer MFSA2024-12 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-12/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-12 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-12/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-15)

QID:	379529
Category:	Local
Associated CVEs:	CVE-2024-29944, CVE-2024-29943
Vendor Reference:	MFSA2024-15

Bugtraq ID:	-
Service Modified:	08/17/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-29943: Out-of-bounds access via Range Analysis bypass
CVE-2024-29944: Privileged JavaScript Execution via Event Handlers

Affected Products:
Prior to Firefox 124.0.1

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 124.0.1 to fix vulnerability, you can also refer MFSA2024-15 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-15 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2024-29943
Description:	bjrjk/CVE-2024-29943 exploit repository
Link:	https://github.com/bjrjk/CVE-2024-29943

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-18)

QID:	379667
Category:	Local
Associated CVEs:	CVE-2024-3859, CVE-2024-3854, CVE-2024-3855, CVE-2024-3302, CVE-2024-3858, CVE-2024-3865, CVE-2024-3852, CVE-2024-3856, CVE-2024-3861, CVE-2024-3860, CVE-2024-3862, CVE-2024-3863, CVE-2024-3857, CVE-2024-3864, CVE-2024-3853
Vendor Reference:	MFSA2024-18
Bugtraq ID:	-
Service Modified:	08/16/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Mozilla has released a security Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to Multiple CVE's
CVE-2024-3859 : Integer-overflow led to out-of-bounds-read in the OpenType sanitizer
CVE-2024-3854 : Out-of-bounds-read after mis-optimized switch statement
CVE-2024-3855 : Incorrect JIT optimization of MSubstr leads to out-of-bounds reads
CVE-2024-3302 : Denial of Service using HTTP/2 CONTINUATION frames
CVE-2024-3858 : Corrupt pointer dereference in js::CheckTracedThing
CVE-2024-3865 : Memory safety bugs fixed in Firefox 125
CVE-2024-3852 : GetBoundName in the JIT returned the wrong object
CVE-2024-3856 : Use-after-free in WASM garbage collection
CVE-2024-3861 : Potential use-after-free due to AlignedBuffer self-move
CVE-2024-3860 : Crash when tracing empty shape lists
CVE-2024-3862 : Potential use of uninitialized memory in MarkStack assignment operator on self-assignment
CVE-2024-3863 : Download Protections were bypassed by .xrm-ms files on Windows
CVE-2024-3857 : Incorrect JITting of arguments led to use-after-free during garbage collection
CVE-2024-3864 : Memory safety bug fixed in Firefox 125, Firefox ESR 115.10, and Thunderbird 115.10
CVE-2024-3853 : Use-after-free if garbage collection runs during realm initialization

Affected Products:
Prior to Firefox 125.0.0.0

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 125 to fix vulnerability, you can also refer MFSA2024-18 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-18/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-18 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-18/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-21)

QID:	379808
Category:	Local
Associated CVEs:	CVE-2024-4775, CVE-2024-4777, CVE-2024-4367, CVE-2024-4770, CVE-2024-4771, CVE-2024-4778, CVE-2024-4768, CVE-2024-4772, CVE-2024-4765, CVE-2024-4769, CVE-2024-4766, CVE-2024-4774, CVE-2024-4773, CVE-2024-4776, CVE-2024-4767, CVE-2024-4764
Vendor Reference:	MFSA2024-21
Bugtraq ID:	-
Service Modified:	09/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-4764: Use-after-free when audio input connected with multiple consumers
CVE-2024-4367: Arbitrary JavaScript execution in PDF.js
CVE-2024-4765: Web application manifests could have been overwritten via hash collision
CVE-2024-4766: Fullscreen notification could have been obscured on Firefox for Android
CVE-2024-4767: IndexedDB files retained in private browsing mode
CVE-2024-4768: Potential permissions request bypass via clickjacking
CVE-2024-4769: Cross-origin responses could be distinguished between script and non-script content-types
CVE-2024-4770: Use-after-free could occur when printing to PDF
CVE-2024-4771: Failed allocation could lead to use-after-free
CVE-2024-4772: Use of insecure rand() function to generate nonce
CVE-2024-4773: URL bar could be cleared after network error
CVE-2024-4774: Undefined behavior in ShmemCharMapHashEntry()
CVE-2024-4775: Invalid memory access in the built-in profiler
CVE-2024-4776: Window may remain disabled after file dialog is shown in full-screen
CVE-2024-4777: Memory safety bugs fixed in Firefox 126, Firefox ESR 115.11, and Thunderbird 115.11
CVE-2024-4778: Memory safety bugs fixed in Firefox 126

Affected Products:
Prior to Firefox 126

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 126 to fix vulnerability, you can also refer MFSA2024-21 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-21/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-21/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2024-4367
Description: LOURC0D3/CVE-2024-4367-PoC exploit repository
Link: https://github.com/LOURC0D3/CVE-2024-4367-PoC

Reference: CVE-2024-4367
Description: s4vvysec/CVE-2024-4367-POC exploit repository
Link: https://github.com/s4vvysec/CVE-2024-4367-POC

Reference: CVE-2024-4367
Description: Zombie-Kaiser/cve-2024-4367-PoC-fixed exploit repository
Link: https://github.com/Zombie-Kaiser/cve-2024-4367-PoC-fixed

Reference: CVE-2024-4367
Description: UnHackerEnCapital/PDFernetRemotelo exploit repository
Link: https://github.com/UnHackerEnCapital/PDFernetRemotelo

Reference: CVE-2024-4367
Description: Masamuneee/CVE-2024-4367-Analysis exploit repository
Link: https://github.com/Masamuneee/CVE-2024-4367-Analysis

gist

Reference: CVE-2024-4367
Description: CVE-2024-4367 Example
Link: https://gist.github.com/FrankSpierings/4579d060d138de67f1f3dc58ff191753

blogs

Reference: CVE-2024-4367
Description: CVE-2024-4367 - Arbitrary JavaScript execution in PDF.js
Link: https://codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js/

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	CVE-2024-4367
Type:	Exploit
Platform:	Document

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-25)

QID:	379936
Category:	Local
Associated CVEs:	CVE-2024-5699, CVE-2024-5687, CVE-2024-5692, CVE-2024-5690, CVE-2024-5698, CVE-2024-5697, CVE-2024-5700, CVE-2024-5689, CVE-2024-5691, CVE-2024-5695, CVE-2024-5694, CVE-2024-5696, CVE-2024-5693, CVE-2024-5701, CVE-2024-5688
Vendor Reference:	MFSA2024-25
Bugtraq ID:	-
Service Modified:	08/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-5687: An incorrect principal could have been used when opening new tabs
CVE-2024-5688: Use-after-free in JavaScript object transplant
CVE-2024-5689: User confusion and possible phishing vector via Firefox Screenshots
CVE-2024-5690: External protocol handlers leaked by timing attack
CVE-2024-5691: Sandboxed iframes were able to bypass sandbox restrictions to open a new window
CVE-2024-5692: Bypass of file name restrictions during saving
CVE-2024-5693: Cross-Origin Image leak via Offscreen Canvas
CVE-2024-5694: Use-after-free in JavaScript Strings
CVE-2024-5695: Memory Corruption using allocation using out-of-memory conditions
CVE-2024-5696: Memory Corruption in Text Fragments
CVE-2024-5697: Website was able to detect when Firefox was taking a screenshot of them
CVE-2024-5698: Data-list could have overlaid address bar
CVE-2024-5699: Cookie prefixes not treated as case-sensitive
CVE-2024-5700: Memory safety bugs fixed in Firefox 127, Firefox ESR 115.12, and Thunderbird 115.12
CVE-2024-5701: Memory safety bugs fixed in Firefox 127

Affected Products:
Prior to Firefox 127

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 127 to fix vulnerability, you can also refer MFSA2024-25 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-25/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-25 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-25/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-29)

QID:	380162
Category:	Local
Associated CVEs:	CVE-2024-6615, CVE-2024-6601, CVE-2024-6603, CVE-2024-6606, CVE-2024-6608, CVE-2024-6602, CVE-2024-6609, CVE-2024-6613, CVE-2024-6612, CVE-2024-6614, CVE-2024-6610, CVE-2024-6611, CVE-2024-6605, CVE-2024-6607, CVE-2024-6604, CVE-2024-6600
Vendor Reference:	MFSA2024-29
Bugtraq ID:	-
Service Modified:	07/12/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-6605: Firefox Android missed activation delay to prevent tapjacking
CVE-2024-6606: Out-of-bounds read in clipboard component
CVE-2024-6607: Leaving pointerlock by pressing the escape key could be prevented
CVE-2024-6608: Cursor could be moved out of the viewport using pointerlock.
CVE-2024-6609: Memory corruption in NSS
CVE-2024-6610: Form validation popups could block exiting full-screen mode
CVE-2024-6600: Memory corruption in WebGL API
CVE-2024-6601: Race condition in permission assignment
CVE-2024-6602: Memory corruption in NSS
CVE-2024-6603: Memory corruption in thread creation
CVE-2024-6611: Incorrect handling of SameSite cookies
CVE-2024-6612: CSP violation leakage when using devtools
CVE-2024-6613: Incorrect listing of stack frames
CVE-2024-6614: Incorrect listing of stack frames
CVE-2024-6604: Memory safety bugs fixed in Firefox 128, Firefox ESR 115.13, and Thunderbird 115.13
CVE-2024-6615: Memory safety bugs fixed in Firefox 128

Affected Products:
Prior to Firefox 128

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 128 to fix vulnerability, you can also refer MFSA2024-29 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-29/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-29 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-29/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-33)

QID:	380283
Category:	Local
Associated CVEs:	CVE-2024-8900, CVE-2024-7519, CVE-2024-7523, CVE-2024-7528, CVE-2024-7527, CVE-2024-7522, CVE-2024-7529, CVE-2024-7518, CVE-2024-7526, CVE-2024-7521, CVE-2024-7531, CVE-2024-7524, CVE-2024-7530, CVE-2024-7525, CVE-2024-7520
Vendor Reference:	MFSA2024-33
Bugtraq ID:	-
Service Modified:	09/18/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-7518: Fullscreen notification dialog can be obscured by document content
CVE-2024-7519: Out of bounds memory access in graphics shared memory handling
CVE-2024-7520: Type confusion in WebAssembly
CVE-2024-7521: Incomplete WebAssembly exception handing
CVE-2024-7522: Out of bounds read in editor component
CVE-2024-7523: Document content could partially obscure security prompts
CVE-2024-7524: CSP strict-dynamic bypass using web-compatibility shims
CVE-2024-7525: Missing permission check when creating a StreamFilter
CVE-2024-7526: Uninitialized memory used by WebGL
CVE-2024-7527: Use-after-free in JavaScript garbage collection
CVE-2024-7528: Use-after-free in IndexedDB
CVE-2024-7529: Document content could partially obscure security prompts
CVE-2024-7530: Use-after-free in JavaScript code coverage collection
CVE-2024-7531: PK11_Encrypt using CKM_CHACHA20 can reveal plaintext on Intel Sandy Bridge machines

Affected Products:
Prior to Firefox 129

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 129 to fix vulnerability, you can also refer MFSA2024-33 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-33/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-33 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-33/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

3 SMB Signing Disabled or SMB Signing Not Required

QID:	90043
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/26/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.

SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.

Please refer to Microsoft's article 887429 (http://support.microsoft.com/kb/887429) and The Basics of SMB Signing (covering both SMB1 and SMB2) (https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2) for information on enabling SMB signing.

For Windows Server 2008 R2, Windows Server 2012, please refer to Microsoft's article Require SMB Security Signatures (http://technet.microsoft.com/en-us/library/cc731957.aspx) for information on enabling SMB signing. For group policies please refer to Microsoft's article Modify Security Policies in Default Domain Controllers Policy (http://technet.microsoft.com/en-us/library/cc731654)

For UNIX systems

To require samba clients running "smbclient" to use packet signing, add the following to the "[global]" section of the Samba configuration file:

client signing = mandatory

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Services\LanManWorkstation\Parameters requiresecuritysignature = 0

3 Allowed Null Session

QID:	90044
Category:	Windows
Associated CVEs:	CVE-2002-1117, CVE-2000-1200
Vendor Reference:	-
Bugtraq ID:	494,959
Service Modified:	06/04/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

It is possible to log into the target host using a NULL session.
Windows NT has a feature allowing anonymous users to obtain domain user names and the share list. Windows NT ACL editor requires the Domain Controllers to return a list of account names.

We check for "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA RestrictAnonymous" as well as "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters RestrictNullSessAccess" = 0 as Microsoft has stated that "Remote access to the registry may still be possible after you follow the steps in this article if the RestrictNullSessAccess registry value has been created and is set to 0. This value allows remote access to the registry by using a null session. The value overrides other explicit restrictive settings."

IMPACT:

Unauthorized users can establish a null session and obtain sensitive information, such as usernames and/or the share list, which could be used in further attacks against the host.

SOLUTION:

To disable or restrict null session, please refer to Microsoft: RestrictNullSessAccess (https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares) for further details.

Please also refer to Microsoft: RestrictAnonymous (https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares) for further details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference:	CVE-2000-1200
Description:	Windows NT allows remote attackers to list all users in a domain by obtaining the domain SID with the LsaQueryInformationPolicy policy function via a null session and using the SID to list the users.
Link:	http://www.securityfocus.com/bid/959

nist-nvd2

Reference:	CVE-2000-1200
Description:	Windows NT allows remote attackers to list all users in a domain by obtaining the domain SID with the LsaQueryInformationPolicy policy function via a null session and using the SID to list the users.
Link:	http://www.securityfocus.com/bid/959

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\ProductOptions ProductType = WinNT
HKLM\SYSTEM\CurrentControlSet\Control\LSA RestrictAnonymous = 0

3 Microsoft Windows VP9 Video Extension Remote Code Execution Vulnerability

QID:	91775
Category:	Windows

Associated CVEs:	CVE-2021-31967
Vendor Reference:	CVE-2021-31967
Bugtraq ID:	-
Service Modified:	08/01/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory.
Microsoft has disclosed Information Disclosure and Remote Code Execution in Windows VP9 Video Extensions.

Affected Product:
VP9 Video Extensions prior to version 1.0.41182.0

IMPACT:

An attacker who successfully exploited this vulnerability could execute arbitrary code on the system.

SOLUTION:

Users are advised to check CVE-2021-31967 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-31967) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-31967 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31967)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'

 3 Microsoft Windows VP9 Video Extension Information Disclosure Vulnerability

QID:	91847
Category:	Windows
Associated CVEs:	CVE-2021-43243
Vendor Reference:	CVE-2021-43243
Bugtraq ID:	-
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft has disclosed Information Disclosure Vulnerability in Windows VP9 Video Extensions.

Affected Product:
VP9 Video Extensions prior to version prior to 1.0.42791.0

IMPACT:

The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.

SOLUTION:

Users are advised to check CVE-2021-43243 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43243) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'

3 Microsoft Office app Remote Code Execution (RCE) Vulnerability

QID:	91850
Category:	Windows
Associated CVEs:	CVE-2021-43905
Vendor Reference:	CVE-2021-43905
Bugtraq ID:	-
Service Modified:	12/29/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Office app is prone to Remote Code Execution Vulnerability.
Affected Software:
App versions prior to 18.2110.13110.0

IMPACT:

Successful exploitation allows attacker to execute arbitrary code.

SOLUTION:

Users are advised to check /CVE-2021-43905 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43905) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-43905 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43905)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Office app detected
Version '18.1903.1152.0'

3 Microsoft Paint 3D Remote Code Execution (RCE) Vulnerability for March 2022

QID:	91871
Category:	Windows
Associated CVEs:	CVE-2022-23282
Vendor Reference:	CVE-2022-23282
Bugtraq ID:	-
Service Modified:	03/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Paint 3D is prone to Remote Code Execution Vulnerability.

IMPACT:

Successful exploitation of the vulnerability may allow remote code execution leading to complete system compromise.

SOLUTION:

Users are advised to refer to CVE-2022-23282 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23282) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.MSPaint detected
Version '6.1907.29027.0'

3 Microsoft Defender Elevation of Privilege Vulnerability for March 2023

QID:	91994
Category:	Windows
Associated CVEs:	CVE-2023-23389
Vendor Reference:	CVE-2023-23389
Bugtraq ID:	-
Service Modified:	03/16/2023
User Modified:	-
Edited:	No

PCI Vuln: Yes

THREAT:

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Affected Software:
Microsoft Malware Protection Engine

IMPACT:

Successful exploitation could allow an attacker to delete data that could include data that results in the service being unavailable.

SOLUTION:

Customers are advised to refer to CVE-2023-23389 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23389) for more information pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-23389 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23389)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

 3 Microsoft Raw Image Extension and VP9 Video Extension Information Disclosure Vulnerability

QID:	92030
Category:	Windows
Associated CVEs:	CVE-2023-36872, CVE-2023-32051
Vendor Reference:	CVE-2023-36872, CVE-2023-32051
Bugtraq ID:	-
Service Modified:	07/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft has disclosed Information Disclosure Vulnerability in Windows VP9 Video Extensions.

Affected Product:
Raw Image Extension Win10 Version 21H2 and 22H2 , Win11 Version 21H2 prior to 2.0.61662.0
Raw Image Extension Win11 Version 22H2 prior to 2.1.61661.0
VP9 Video Extensions prior to 1.0.61591.0

IMPACT:

An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory..

SOLUTION:

Users are advised to check CVE-2023-36872 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36872),CVE-2023-32051 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051)for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-36872 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36872)

CVE-2023-32051 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32051)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft vulnerable Microsoft.VP9VideoExtensions detected
Version '1.0.22681.0'

3 SMBv2 Signing Not Required

QID:	92094
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Server Message Block (SMB) protocol provides the basis for file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets.

Beginning with SMBv2 clients and servers, signing can be either required or not required.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Customers are advised to refer to Microsoft network server: Digitally sign communications (always)

(https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always#default-values)

or Microsoft network client: Digitally sign communications (always)

(https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always)

for more information pertaining to SMBv2 best practices, location, values, policy management and security considerations.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SMB2 Signing not required

3 Microsoft Windows Nearby Sharing Spoofing Vulnerability Security Update for January 2024

QID:	92104
Category:	Windows
Associated CVEs:	CVE-2024-20690
Vendor Reference:	CVE-2024-20690
Bugtraq ID:	-
Service Modified:	01/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft Windows OS Security Update - January 2024

Patch version is 10.0.17763.5329 for KB5034127

(https://support.microsoft.com/en-in/help/5034127)
Patch version is 10.0.22631.3007 for KB5034123

(https://support.microsoft.com/en-in/help/5034123)
Patch version is 10.0.19045.3930 for KB5034122

(https://support.microsoft.com/en-in/help/5034122)
Patch version is 10.0.22000.2713 for KB5034121

(https://support.microsoft.com/en-in/help/5034121)

IMPACT:

Successful exploit could compromise Integrity

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5034127 (https://support.microsoft.com/en-in/help/5034127)
KB5034123 (https://support.microsoft.com/en-in/help/5034123)
KB5034122 (https://support.microsoft.com/en-in/help/5034122)
KB5034121 (https://support.microsoft.com/en-in/help/5034121)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5034121 (https://support.microsoft.com/en-in/help/5034121)

KB5034122 (https://support.microsoft.com/en-in/help/5034122)

KB5034123 (https://support.microsoft.com/en-in/help/5034123)

KB5034127 (https://support.microsoft.com/en-in/help/5034127)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5034122 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.3803

3 Microsoft Defender Security Feature Bypass Vulnerability March 2024

QID:	92123
Category:	Windows
Associated CVEs:	CVE-2024-20671
Vendor Reference:	CVE-2024-20671
Bugtraq ID:	-
Service Modified:	04/03/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Malware Protection Platform is affected by a security feature bypass vulnerability CVE-2024-20671.

Affected Versions / Software:
Microsoft Malware Protection Platform prior to Version 4.18.24010.12

IMPACT:

Successful exploitation of this vulnerability could prevent Microsoft Defender from starting.

SOLUTION:

Users are advised to check CVE-2024-20671 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-20671) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-20671 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-20671)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files\Windows Defender\\ProtectionManagement.dll Version is 4.18.1909.6

3 Microsoft .NET Framework Update for April 2024

QID:	92130
Category:	Windows
Associated CVEs:	CVE-2024-21409
Vendor Reference:	5037034, 5037040, 5037039, 5037127, 5037038, 5036899, 5037033, 5036609, 5037036, 5037035, 5037037, 5037041, 5037128, 5036620
Bugtraq ID:	-
Service Modified:	04/15/2024

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A Remote Code Execution Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
5037034
5037040
5037039
5037127
5037038
5036899
5037033
5036609
5037036
5037035
5037037
5037041
5037128
5036620

This security update is rated Important for supported versions of Microsoft .NET Framework.
.NET Framework 2.0, 3.0, 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation may allow a attacker to perform Remote Code Execution.

SOLUTION:

Customers are advised to refer to CVE-2024-21409 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21409)for more details pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-21409 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21409)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5037036 or KB5037035 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.dll Version is 4.8.4682.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.dll Version is 4.8.4682.0

3 Microsoft .NET Framework Update for July 2024

QID:	92150
Category:	Windows
Associated CVEs:	CVE-2024-38081
Vendor Reference:	5040434, 5041017, 5041020, 5041016, 5041023, 5041022, 5041021, 5041026, 5039885, 5041024, 5041027, 5039895, 5041019, 5041018, 5040448
Bugtraq ID:	-
Service Modified:	07/10/2024
User Modified:	-
Edited:	No

PCI Vuln: Yes

THREAT:

A Remote Code Execution Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
5040448
5040434
5041017
5041020
5041016
5041023
5041022
5041021
5041026
5039885
5041024
5041027
5039895
5041019
5041018

This security update is rated Important for supported versions of Microsoft .NET Framework.
.NET Framework 2.0, 3.0, 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation may allow a attacker to have Elevated Privileges.

SOLUTION:

Customers are advised to refer to CVE-2024-38081 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38081) for more details pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-38081 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38081)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5041018 or KB5041019 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\Mscorlib.dll Version is 4.8.4645.0
%windir%\Microsoft.NET\Framework\v4.0.30319\Mscorlib.dll Version is 4.8.4645.0

3 VLC Media Player Real Demuxer File Handling Array Indexing Vulnerability(VideoLAN-SA-1007, VideoLAN-SA-1101)

QID:	118886
Category:	Local
Associated CVEs:	CVE-2010-3907
Vendor Reference:	VideoLAN-SA-1007, VideoLAN-SA-1101
Bugtraq ID:	45632
Service Modified:	01/25/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC Media Player is prone to a vulnerability caused by an array indexing error in the "Close()" and "DemuxAudioMethod1()" [modules/demux/real.c] functions within the Real demuxer when processing a Real Media file with a zero "i_subpackets" value.

Affected Versions:
VLC Media Player Versions prior to 1.1.6

IMPACT:

If this vulnerability is successfully exploited, attackers can crash an affected application or compromise a vulnerable system by enticing a user into opening a malicious media file or visiting a specially crafted Web page.

SOLUTION:

This issue has been resolved in VLC Media Player 1.1.6 and later. Refer to vendor advisory VideoLAN-SA-1007 (http://www.videolan.org/security/sa1007.html) and VideoLAN-SA-1101 (http://www.videolan.org/security/sa1101.html) to obtain additional details about the vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

SA-1007 (VLC Media Player 1.1.6) (http://git.videolan.org/?p=vlc.git;a=commitdiff;h=6568965770f906d34d4aef83237842a5376adb55;hp=403718957b551c3c27546b7f82b2ae9ba937652f)

SA-1007 (VLC Media Player 1.1.6) (http://cdnetworks-kr-1.dl.sourceforge.net/project/vlc/1.1.6/win32/vlc-1.1.6-win32.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player USF and Text Subtitles Decoders Buffer Overflow

QID:	119265
Category:	Local
Associated CVEs:	CVE-2011-0522
Vendor Reference:	-
Bugtraq ID:	46008
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

Two vulnerabilities have been identified in VLC Media Player.These issues are caused by buffer overflow errors in the StripTags function within the USF and Text subtitles decoders when processing malformed data.

Affected Versions:
VLC Media Player 1.1 before 1.1.6

IMPACT:

If this vulnerability is successfully exploited, attackers can execute arbitrary code.

SOLUTION:

Update to Version 1.1.6 or later to resolve this issue.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC Media Player 1.1.6 (http://download.videolan.org/pub/videolan/vlc/1.1.6/win32/vlc-1.1.6-win32.zip)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2011-0522
- Description: VideoLAN VLC Media Player 1.1 - Subtitle 'StripTags()' Memory Corruption - The Exploit-DB Ref : 16108
- Link: http://www.exploit-db.com/exploits/16108

exploitdb
- Reference: CVE-2011-0522
- Description: VideoLAN VLC Media Player 1.1 - Subtitle 'StripTags()' Memory Corruption
- Link: https://www.exploit-db.com/exploits/16108

nvd
- Reference: CVE-2011-0522
- Description: The StripTags function in (1) the USF decoder (modules/codec/subtitles/subsdec.c) and (2) the Text decoder (modules/codec/subtitles/subsusf.c) in VideoLAN VLC Media Player 1.1 before 1.1.6-rc allows remote attackers to execute arbitrary code via a subtitle with an opening "" in an MKV file, which triggers heap memory corruption, as demonstrated using refined-australia-blu720p-sample.mkv.
- Link: http://www.exploit-db.com/exploits/16108

- Reference: CVE-2011-0522
- Description: The StripTags function in (1) the USF decoder (modules/codec/subtitles/subsdec.c) and (2) the Text decoder (modules/codec/subtitles/subsusf.c) in VideoLAN VLC Media Player 1.1 before 1.1.6-rc allows remote attackers to execute arbitrary code via a subtitle with an opening "" in an MKV file, which triggers heap memory corruption, as demonstrated using refined-australia-blu720p-sample.mkv.
- Link: http://www.securityfocus.com/bid/46008

seebug
- Reference: CVE-2011-0522
- Description: VLC Media Player Subtitle StripTags() Function Memory Corruption
- Link: https://www.seebug.org/vuldb/ssvid-70665

packetstorm
- Reference: CVE-2011-0522
- Description: VLC Media Player Memory Corruption
- Link: https://packetstormsecurity.com/files/98139/VLC-Media-Player-Memory-Corruption.html

white-phosphorus
- Reference: CVE-2011-0522
- Description: wp_vlc_mediaplayer_mkvdemuxer
- Link: http://exploitlist.immunityinc.com/home/exploitpack/White_Phosphorus/wp_vlc_mediaplayer_mkvdemuxer

nist-nvd2
- Reference: CVE-2011-0522
- Description: The StripTags function in (1) the USF decoder (modules/codec/subtitles/subsdec.c) and (2) the Text decoder (modules/codec/subtitles/subsusf.c) in VideoLAN VLC Media Player 1.1 before 1.1.6-rc allows remote attackers to execute arbitrary code via a subtitle with an opening "" in an MKV file, which triggers heap memory corruption, as demonstrated using refined-australia-blu720p-sample.mkv.
- Link: http://www.securityfocus.com/bid/46008

- Reference: CVE-2011-0522
- Description: The StripTags function in (1) the USF decoder (modules/codec/subtitles/subsdec.c) and (2) the Text decoder (modules/codec/subtitles/subsusf.c) in VideoLAN VLC Media Player 1.1 before 1.1.6-rc allows remote attackers to execute arbitrary code via a subtitle with an opening "" in an MKV file, which triggers heap memory corruption, as demonstrated

using refined-australia-blu720p-sample.mkv.

Link: http://www.exploit-db.com/exploits/16108

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player XSPF Demuxer Integer Overflow Vulnerability

QID:	119317
Category:	Local
Associated CVEs:	-
Vendor Reference:	VLC 1.1.10 release
Bugtraq ID:	-
Service Modified:	06/07/2011
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

An integer overflow vulnerability exists in VLC Media Player. The vulnerability is within the XPSF demuxer. Further details are not available at this time.

Affected Versions:
VLC Media Player versions prior to 1.1.10

IMPACT:

If this vulnerability is successfully exploited, attackers can execute arbitrary code.

SOLUTION:

Update to Version 1.1.10 to resolve this issue. The latest version is available for download fromVLC Media Player Web site (http://www.videolan.org/vlc/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC Media Player 1.1.10: Windows (http://cdnetworks-kr-1.dl.sourceforge.net/project/vlc/1.1.10/win32/vlc-1.1.10-win32.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player Heap Based Buffer Overflow Vulnerability (VideoLAN-SA-1107)

QID:	119635
Category:	Local

Associated CVEs:	-
Vendor Reference:	VideoLAN-SA-1107
Bugtraq ID:	50007
Service Modified:	05/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC is a cross-platform media player.

The application is prone to a heap-based memory corruption vulnerability because it fails to properly bounds check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue occurs due to an NULL pointer dereference error in the "httpd_ClientRecv" function of the "src/network/httpd.c" source file. The issue affects the "HTTP" and "RTSP" server components.

Affected Versions:
VLC media player 1.1.11 and earlier

IMPACT:

If this vulnerability is successfully exploited, attackers can crash the affected application, denying service to legitimate users.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to Security Advisory 1107 (http://www.videolan.org/security/sa1107.html) to obtain additional details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Security Advisory 1107: Windows (http://www.videolan.org/security/sa1107.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

 3 VLC Media Player Multiple Remote Code Execution Vulnerabilities (VideoLAN-SA-1201) (VideoLAN-SA-1202)

QID:	120497
Category:	Local
Associated CVEs:	CVE-2012-1775, CVE-2012-1776
Vendor Reference:	VideoLAN-SA-1201, VideoLAN-SA-1202
Bugtraq ID:	52550,53391
Service Modified:	08/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

The application is prone to multiple memory corruption vulnerabilities due to improper bounds checks on user-supplied data by the implemented

"MMS" and "Real RTSP" components of the affected software versions.Specifically, the function MMSOpen() used by the MMS access plugin encounters a stack-based buffer overflow when processing maliciously crafted MMS streams because of improper boundary validation. (CVE-2012-1775). The Real RTSP plugin also could allow remote code execution or a denial of service when processing maliciously crafted Real RTSP streams. (CVE-2012-1776)

An attacker could provide a specially crafted link that directs a user to a malicious site by using misleading language or instructions to convince the user to follow the provided link.
Affected Versions:
VLC media player 2.0.1 and earlier

IMPACT:

A successful exploit allows an attacker to execute arbitrary code or cause a denial of service on a targeted operating system.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to Security Advisory 1201 (http://www.videolan.org/security/sa1201.html) or Security Advisory 1202 (http://www.videolan.org/security/sa1202.html) to obtain additional details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN VLC Player 2.0.1 (http://www.videolan.org/vlc/#download)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security
- Reference: CVE-2012-1775
- Description: VLC MMS Stream Handling Buffer Overflow Exploit - Core Security Category : Exploits/Client Side

Metasploit
- Reference: CVE-2012-1775
- Description: VLC MMS Stream Handling Buffer Overflow - Metasploit Ref : /modules/exploit/windows/browser/vlc_mms_bof
- Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/vlc_mms_bof.rb

The Exploit-DB
- Reference: CVE-2012-1775
- Description: VideoLAN VLC Media Player 2.0.0 - Mms Stream Handling Buffer Overflow (Metasploit) - The Exploit-DB Ref : 18825
- Link: http://www.exploit-db.com/exploits/18825

exploitdb
- Reference: CVE-2012-1775
- Description: VideoLAN VLC Media Player 2.0.0 - Mms Stream Handling Buffer Overflow (Metasploit)
- Link: https://www.exploit-db.com/exploits/18825

seebug
- Reference: CVE-2012-1775
- Description: VLC MMS Stream Handling Buffer Overflow
- Link: https://www.seebug.org/vuldb/ssvid-72853

saint
- Reference: CVE-2012-1775
- Description: VideoLAN VLC Media Player MMS URI Stack Overflow
- Link: https://my.saintcorporation.com/cgi-bin/exploit_info/vlc_mms_uri_overflow

packetstorm
- Reference: CVE-2012-1775
- Description: VLC MMS Stream Handling Buffer Overflow
- Link: https://packetstormsecurity.com/files/112442/VLC-MMS-Stream-Handling-Buffer-Overflow.html

metasploit
- Reference: CVE-2012-1775
- Description: VLC MMS Stream Handling Buffer Overflow
- Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2012-1775
Description: VLC MMS Stream Handling Buffer Overflow
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/vlc_mms_bof.rb

coreimpact
Reference: CVE-2012-1775
Description: VLC MMS Stream Handling Buffer Overflow Exploit Update
Link: https://www.coresecurity.com/core-labs/exploits

nist-nvd2
Reference: CVE-2012-1775
Description: Stack-based buffer overflow in VideoLAN VLC media player before 2.0.1 allows remote attackers to execute arbitrary code via a crafted MMS:// stream.
Link: http://www.exploit-db.com/exploits/18825

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player .swf File Processing Denial of Service Vulnerability

QID:	120720
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

The application is vulnerable to a buffer overflow condition that occurs during the processing of context specific .swf files. Though the publicly available proof-of-concept code suggests that arbitrary code execution is possible, it has not been proven.

An attacker could provide a specially crafted link that directs a user to a malicious site by using misleading language or instructions to convince the user to follow the provided link.

The affected application is not a default application for processing .swf files. This reduces the probability of a successful exploit.

Affected Versions:
VLC media player 2.0.4 and earlier

IMPACT:

A successful exploit allows an attacker to cause a denial of service on a targeted operating system.

SOLUTION:

The vendor has not confirmed the vulnerability or released updates to resolve this issue.

Workaround:
Users are advised to avoid processing of .swf files with the affected application until updates are available.
Administrators may contact the vendor for information regarding patches and updates pertaining to this vulnerability.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player PNG File Processing Denial of Service Vulnerability

QID:	120724
Category:	Local
Associated CVEs:	CVE-2012-5470
Vendor Reference:	VideoLAN-SA-1203
Bugtraq ID:	55850
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

The application is vulnerable to a buffer overflow condition that occurs during the parsing of malicious PNG files, leading to a crash of the process of the VLC media player.

An attacker could provide a specially crafted link that directs a user to a malicious site by using misleading language or instructions to convince the user to follow the provided link.

The affected application is not a default application for processing PNG files. This reduces the probability of a successful exploit.

Affected Versions:
VLC media player 2.0.3 and earlier

IMPACT:

A successful exploit allows an attacker to cause a denial of service on a targeted operating system.

SOLUTION:

The vendor has confirmed the vulnerability and released VLC media player version 2.0.4 to resolve this issue that can be downloaded from here (http://www.videolan.org/vlc/download-windows.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1203: Windows (http://www.videolan.org/vlc/download-windows.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2012-5470
- Description: VideoLAN VLC Media Player 2.0.3 - '.png' ReadAV Crash (PoC) - The Exploit-DB Ref : 21889
- Link: http://www.exploit-db.com/exploits/21889

exploitdb
- Reference: CVE-2012-5470
- Description: VideoLAN VLC Media Player 2.0.3 - '.png' ReadAV Crash (PoC)
- Link: https://www.exploit-db.com/exploits/21889

nvd
- Reference: CVE-2012-5470
- Description: libpng_plugin in VideoLAN VLC media player 2.0.3 allows remote attackers to cause a denial of service (application crash) via a crafted PNG file.

Link: http://www.exploit-db.com/exploits/21889/

seebug
Reference: CVE-2012-5470
Description: VLC Player
Link: https://www.seebug.org/vuldb/ssvid-75707

nist-nvd2
Reference: CVE-2012-5470
Description: libpng_plugin in VideoLAN VLC media player 2.0.3 allows remote attackers to cause a denial of service (application crash) via a crafted PNG file.
Link: http://www.exploit-db.com/exploits/21889/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player Playlist File Denial of Service Vulnerability

QID:	121859
Category:	Local
Associated CVEs:	CVE-2013-7340
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

A denial of service vulnerability exists in VLC, which can be exploited remotely by an attacker using a maliciously crafted playlist file that increases the memory consumption, causing the application to crash.

Affected Versions:
VLC prior to version 2.0.7

IMPACT:

Successful exploitation of this vulnerability will cause the application to crash

SOLUTION:

Users are advised to upgrade to the lastest version of the software available.Latest version can be downloaded from VLC (http://www.videolan.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player Memory Corruption Vulnerability

QID:	122073
Category:	Local
Associated CVEs:	CVE-2014-3441
Vendor Reference:	-
Bugtraq ID:	67315
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

A memory corruption vulnerability has been reported in the application which exist as the application fails to perform proper boundary verification when playing certain file types.The vulnerability is exploitable via a malformed .png file which loads codec\libpng_plugin.dll.

Affected Versions:
VLC 2.1.3, prior versions may be affected.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code in the context of user using affected version of the software.Failed exploits may result in denial of service.

SOLUTION:

Customers are advised to update to the lastest version of VLC Media Player (http://www.videolan.org/vlc/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Bug 1080606: VLC media player (http://www.videolan.org/vlc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2014-3441
- Description: VideoLAN VLC Media Player 2.1.3 - '.wav' File Memory Corruption - The Exploit-DB Ref : 39177
- Link: http://www.exploit-db.com/exploits/39177

Qualys
- Reference: CVE-2014-3441
- Description: VLC Media Player 2.1.3 Memory Corruption Vulnerability
- Link: http://packetstormsecurity.com/files/126564/VLC-Player-2.1.3-Memory-Corruption.html

exploitdb
- Reference: CVE-2014-3441
- Description: VideoLAN VLC Media Player 2.1.3 - '.wav' File Memory Corruption
- Link: https://www.exploit-db.com/exploits/39177

nvd
- Reference: CVE-2014-3441
- Description: codec\libpng_plugin.dll in VideoLAN VLC Media Player 2.1.3 allows remote attackers to cause a denial of service (crash) via a

crafted .png file, as demonstrated by a png in a .wave file.

Link: http://www.securityfocus.com/bid/67315

Reference: CVE-2014-3441
Description: codec\libpng_plugin.dll in VideoLAN VLC Media Player 2.1.3 allows remote attackers to cause a denial of service (crash) via a crafted .png file, as demonstrated by a png in a .wave file.
Link: http://packetstormsecurity.com/files/126564/VLC-Player-2.1.3-Memory-Corruption.html

packetstorm
Reference: CVE-2014-3441
Description: VLC Player 2.1.3 Memory Corruption
Link: https://packetstormsecurity.com/files/126564/VLC-Player-2.1.3-Memory-Corruption.html

nist-nvd2
Reference: CVE-2014-3441
Description: codec\libpng_plugin.dll in VideoLAN VLC Media Player 2.1.3 allows remote attackers to cause a denial of service (crash) via a crafted .png file, as demonstrated by a png in a .wave file.
Link: http://packetstormsecurity.com/files/126564/VLC-Player-2.1.3-Memory-Corruption.html

Reference: CVE-2014-3441
Description: codec\libpng_plugin.dll in VideoLAN VLC Media Player 2.1.3 allows remote attackers to cause a denial of service (crash) via a crafted .png file, as demonstrated by a png in a .wave file.
Link: http://www.securityfocus.com/bid/67315

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player GnuTLS "read_server_hello()" Memory Corruption Vulnerability

QID:	122327
Category:	Local
Associated CVEs:	CVE-2014-3466, CVE-2014-0333
Vendor Reference:	VLC
Bugtraq ID:	67741
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

A memory corruption vulnerability has been reported in the application which exist as the application fails to perform proper boundary verification when playing certain file types.

Affected Versions:
VLC 2.1.4, prior versions may be affected.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code, failed exploits may result in denial of service

SOLUTION:

Users are advised to upgrade to the latest version of the software available.Latest version can be obtained from VLC (http://www.videolan.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC: Windows (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2014-3466
Description: Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.
Link: https://www.gitorious.org/gnutls/gnutls/commit/688ea6428a432c39203d00acd1af0e7684e5ddfd

Reference: CVE-2014-3466
Description: Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.
Link: http://radare.today/technical-analysis-of-the-gnutls-hello-vulnerability/

nist-nvd2

Reference: CVE-2014-3466
Description: Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.
Link: http://radare.today/technical-analysis-of-the-gnutls-hello-vulnerability/

Reference: CVE-2014-3466
Description: Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.
Link: https://www.gitorious.org/gnutls/gnutls/commit/688ea6428a432c39203d00acd1af0e7684e5ddfd

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player HTML Subtitle and Freetype Renderer Buffer Overflow Vulnerabilities

QID:	122478
Category:	Local
Associated CVEs:	CVE-2013-1868
Vendor Reference:	VideoLAN-SA-1301
Bugtraq ID:	57079
Service Modified:	05/28/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project. A vulnerability exists in the HTML subtitle and freetype renderer module of the affected software because of an invalid memory access condition.

Affected Software:
VLC media player 2.0.4 and earlier

IMPACT:

Successful exploitation could allow an unauthenticated, remote attacker to cause a buffer overflow condition or cause a denial of service on the affected system.

SOLUTION:

Customers are advised to install VLC media player 2.0.5 (http://www.videolan.org/) or later to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC media player 2.0.5 or later: Windows (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2013-1868
Description: VideoLAN VLC Media Player 2.0.4 - '.swf' Crash (PoC) - The Exploit-DB Ref : 23201
Link: http://www.exploit-db.com/exploits/23201

exploitdb
Reference: CVE-2013-1868
Description: VideoLAN VLC Media Player 2.0.4 - '.swf' Crash (PoC)
Link: https://www.exploit-db.com/exploits/23201

seebug
Reference: CVE-2013-1868
Description: VLC Media Player 2.0.4 (.swf) - Crash PoC
Link: https://www.seebug.org/vuldb/ssvid-76977

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media Player ".asf" File Denial of Service Vulnerability

QID:	122728
Category:	Local
Associated CVEs:	CVE-2014-1684
Vendor Reference:	CVE-2014-1684
Bugtraq ID:	65399
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

A division by zero error exist in the ASF_ReadObject_file_properties function of modules/demux/asf/libasf.c souce file used within ASF Demuxer. An attacker could exploit this vulnerability by persuading a user to open a crafted ASF file with zero minimum and maximum data packet size in the file property header.

Affected Versions:
VideoLAN VLC Media Player before 2.1.3 are affected.

IMPACT:

Successful exploitation could allow an unauthenticated, remote attacker to trigger a divide-by-zero error and cause a denial of service condition on the affected system.

SOLUTION:

Customers are advised to install VLC media player 2.1.3 or later (http://www.videolan.org/) to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC media player 2.1.3 or later (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2014-1684
- Description: VideoLAN VLC Media Player 2.1.2 - '.asf' Crash (PoC) - The Exploit-DB Ref : 31429
- Link: http://www.exploit-db.com/exploits/31429

Qualys
- Reference: CVE-2014-1684
- Description: VLC ASF Demuxer Division By Zero Bug
- Link: http://www.elsherei.com/?p=269

exploitdb
- Reference: CVE-2014-1684
- Description: VideoLAN VLC Media Player 2.1.2 - '.asf' Crash (PoC)
- Link: https://www.exploit-db.com/exploits/31429

nvd
- Reference: CVE-2014-1684
- Description: The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media Player before 2.1.3 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero minimum and maximum data packet size in an ASF file.
- Link: https://trac.videolan.org/vlc/ticket/10482

- Reference: CVE-2014-1684
- Description: The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media Player before 2.1.3 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero minimum and maximum data packet size in an ASF file.
- Link: http://git.videolan.org/gitweb.cgi/vlc.git/?p=vlc.git;a=commitdiff;h=98787d0843612271e99d62bee0dfd8197f0cf404

- Reference: CVE-2014-1684
- Description: The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media Player before 2.1.3 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero minimum and maximum data packet size in an ASF file.
- Link: http://www.elsherei.com/?p=269

packetstorm
- Reference: CVE-2014-1684
- Description: VLC Media Player 2.1.2 Denial Of Service
- Link: https://packetstormsecurity.com/files/125080/VLC-Media-Player-2.1.2-Denial-Of-Service.html

0day.today
- Reference: CVE-2014-1684
- Description: VLC 2.1.2 (.asf) - Crash PoC
- Link: https://0day.today/exploit/21864

nist-nvd2
- Reference: CVE-2014-1684
- Description: The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media Player before 2.1.3 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero minimum and maximum data packet size in an ASF file.
- Link: http://www.elsherei.com/?p=269

- Reference: CVE-2014-1684
- Description: The ASF_ReadObject_file_properties function in modules/demux/asf/libasf.c in the ASF Demuxer in VideoLAN VLC Media Player before 2.1.3 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a zero minimum and maximum data packet size in an ASF file.
- Link: https://trac.videolan.org/vlc/ticket/10482

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player Multiple Memory Corruption Vulnerabilities

QID:	123164
Category:	Local
Associated CVEs:	CVE-2014-9597, CVE-2014-9598
Vendor Reference:	VLC
Bugtraq ID:	-
Service Modified:	05/29/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

Multiple memory corruption vulnerability have been reported in the application which exist as the application fails to properly sanitized user-supplied input when handling some specially crafted FLV and M2V file

Affected Versions:
VLC Player 2.1.5, prior versions may be affected.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code, failed exploits may result in denial of service.

SOLUTION:

The vendor has confirmed the vulnerability however there is no patch available as of now.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2014-9597
Description:	VideoLAN VLC Media Player 2.1.5 - DEP Access Violation - The Exploit-DB Ref : 35901
Link:	http://www.exploit-db.com/exploits/35901
Reference:	CVE-2014-9598
Description:	VideoLAN VLC Media Player 2.1.5 - Write Access Violation - The Exploit-DB Ref : 35902
Link:	http://www.exploit-db.com/exploits/35902

exploitdb

Reference:	CVE-2014-9597
Description:	VideoLAN VLC Media Player 2.1.5 - DEP Access Violation
Link:	https://www.exploit-db.com/exploits/35901
Reference:	CVE-2014-9598
Description:	VideoLAN VLC Media Player 2.1.5 - Write Access Violation
Link:	https://www.exploit-db.com/exploits/35902

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player "m3u8/m3u" Denial of Service Vulnerability

QID:	123844
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

A denial of service vulnerability have been reported in the application which exist as the application fails to properly handling some specially crafted m3u8/m3u file

Affected Versions:
VLC Player 2.2.1, prior versions may be affected.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to cause a denial of service

SOLUTION:

The vendor has not confirmed the vulnerability and no patch information is available as of now

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media Player Buffer Overflow Vulnerability (VideoLAN-SA-1601)

QID:	370054
Category:	Local
Associated CVEs:	CVE-2016-5108
Vendor Reference:	VideoLAN-SA-1601
Bugtraq ID:	90924
Service Modified:	05/29/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

A remote user can create a specially crafted QuickTime IMA file that, when loaded by the target user, will trigger a buffer overflow in DecodeAdpcmImaQT() in 'modules/codec/adpcm.c'.

Affected Version
VLC media player 2.2.3 and earlier

IMPACT:

On successful exploitation it allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted QuickTime IMA file.

SOLUTION:

The vendor has confirmed the vulnerability and advised to upgrade to newer version. Latest version can be downloaded from VLC media player (http://www.videolan.org/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

SA1601: Windows (https://www.videolan.org/security/sa1601.html)

SA1601: MAC OS X (https://www.videolan.org/security/sa1601.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2016-5108
- Description: VideoLAN VLC Media Player 2.2.1 - 'DecodeAdpcmImaQT' Buffer Overflow - The Exploit-DB Ref : 41025
- Link: http://www.exploit-db.com/exploits/41025

exploitdb
- Reference: CVE-2016-5108
- Description: VideoLAN VLC Media Player 2.2.1 - 'DecodeAdpcmImaQT' Buffer Overflow
- Link: https://www.exploit-db.com/exploits/41025

packetstorm
- Reference: CVE-2016-5108
- Description: VideoLan VLC Media Player 2.2.1 Buffer Overflow
- Link: https://packetstormsecurity.com/files/140464/VideoLan-VLC-Media-Player-2.2.1-Buffer-Overflow.html

0day.today
- Reference: CVE-2016-5108
- Description: VideoLAN VLC Media Player 2.2.1 - DecodeAdpcmImaQT Buffer Overflow Exploit
- Link: https://0day.today/exploit/26652

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media Player Arbitrary Code Execution Vulnerability

QID:	371114
Category:	Local
Associated CVEs:	CVE-2018-11529
Vendor Reference:	VLC
Bugtraq ID:	-
Service Modified:	02/28/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

VLC media player through 2.2.8 is prone to a Use-After-Free (UAF) vulnerability. This issue allows an attacker to execute arbitrary code in the context of the logged-in user via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.

Affected Version:
VLC Media Player versions through 2.2.8

IMPACT:

On successful exploitation it allows attackers to execute arbitrary commands on the system.

SOLUTION:

Currently there is no information about possible countermeasures. For future reference and latest download , please visit VLC Media Player (https://get.videolan.org/vlc/3.0.3/win64/vlc-3.0.3-win64.exe).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC 4.0.3 (https://www.videolan.org/vlc/releases/3.0.3.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit
- Reference: CVE-2018-11529
- Description: VLC Media Player MKV Use After Free - Metasploit Ref : /modules/exploit/windows/fileformat/vlc_mkv
- Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/fileformat/vlc_mkv.rb

The Exploit-DB
- Reference: CVE-2018-11529
- Description: VLC Media Player - MKV Use-After-Free (Metasploit) - The Exploit-DB Ref : 45626
- Link: http://www.exploit-db.com/exploits/45626

Qualys
- Reference: CVE-2018-11529
- Description: VLC media player 2.2.8 Arbitrary Code Execution PoC
- Link: http://seclists.org/fulldisclosure/2018/Jul/28

exploitdb
- Reference: CVE-2018-11529
- Description: VLC Media Player - MKV Use-After-Free (Metasploit)
- Link: https://www.exploit-db.com/exploits/45626

nvd
- Reference: CVE-2018-11529
- Description: VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.
- Link: https://www.exploit-db.com/exploits/45626/

- Reference: CVE-2018-11529
- Description: VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.
- Link: http://seclists.org/fulldisclosure/2018/Jul/28

seebug
- Reference: CVE-2018-11529
- Description: VLC media player 2.2.8 Arbitrary Code Execution PoC(CVE-2018-11529)
- Link: https://www.seebug.org/vuldb/ssvid-97416

packetstorm
- Reference: CVE-2018-11529
- Description: VLC Media Player 2.2.8 MKV Use-After-Free
- Link: https://packetstormsecurity.com/files/149759/VLC-Media-Player-2.2.8-MKV-Use-After-Free.html

Reference: CVE-2018-11529
Description: VLC Media Player 2.2.8 Arbitrary Code Execution
Link: https://packetstormsecurity.com/files/148471/VLC-Media-Player-2.2.8-Arbitrary-Code-Execution.html

metasploit
Reference: CVE-2018-11529
Description: VLC Media Player MKV Use After Free
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2018-11529
Description: VLC Media Player MKV Use After Free
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/fileformat/vlc_mkv.rb

0day.today
Reference: CVE-2018-11529
Description: VLC Media Player 2.2.8 MKV Use-After-Free Exploit
Link: https://0day.today/exploit/31299

Reference: CVE-2018-11529
Description: VLC Media Player - MKV Use-After-Free Exploit
Link: https://0day.today/exploit/31351

nist-nvd2
Reference: CVE-2018-11529
Description: VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.
Link: https://www.exploit-db.com/exploits/45626/

Reference: CVE-2018-11529
Description: VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.
Link: http://seclists.org/fulldisclosure/2018/Jul/28

ASSOCIATED MALWARE:
ReversingLabs
Malware ID: CVE-2018-11529
Type: Exploit
Platform: Win32

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media Player Multiple Security Vulnerabilities (VideoLAN-SA-1901)

QID:	371832
Category:	Local
Associated CVEs:	CVE-2019-5439, CVE-2019-12874, CVE-2019-5459
Vendor Reference:	VideoLAN-SA-1901
Bugtraq ID:	108769,108882
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.

A total of 33 vulnerabilities were fixed in the release of VLC 3.0.7. Two problems received the status of highly dangerous, 21 bugs are rated as medium, and another 20 vulnerabilities are considered low-risk.

Affected Version:
VLC Media Player versions through 3.0.6

IMPACT:

On successful exploitation it allows attackers to execute out-of-bound write vulnerability, heap overflows, NULL-dereference and use-after-free security issues.

SOLUTION:

Installing a new version of the player, for obvious reasons, is highly recommended to all VLC users. The full list of changes in VLC 3.0.7 can be seen here (https://www.videolan.org/developers/vlc-branch/NEWS).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC 3.0.7 (https://www.videolan.org/vlc/releases/3.0.7.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-5459
Description: An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.
Link: https://hackerone.com/reports/502816

nist-nvd2

Reference: CVE-2019-5459
Description: An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.
Link: https://hackerone.com/reports/502816

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC media player Remote Code Execution Vulnerability(VideoLAN-SB-VLC-308)

QID:	372080
Category:	Local
Associated CVEs:	CVE-2019-13602, CVE-2019-13962, CVE-2019-14437, CVE-2019-14438, CVE-2019-14498, CVE-2019-14533, CVE-2019-14534, CVE-2019-14535, CVE-2019-14776, CVE-2019-14777, CVE-2019-14778, CVE-2019-14970
Vendor Reference:	VideoLAN-SB-VLC-308
Bugtraq ID:	109158,109306
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

LC media player is a portable, free and open-source, cross-platform media player and streaming media server written by the VideoLAN project.A remote user could create a specifically crafted file that could trigger issues ranging from buffer overflows to division by zero.

Affected Version:VideoLAN VLC media player prior to 3.0.8

IMPACT:

A remote user could create a specifically crafted file that could trigger issues ranging from buffer overflows to division by zero.

SOLUTION:

Upgrade to the latest packages which contain a patch. Refer to VideoLAN-SB-VLC-308 (https://www.videolan.org/security/sb-vlc308.html) for details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-308 (https://www.videolan.org/security/sb-vlc308.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference:	CVE-2019-13962
Description:	lavc_CopyPicture in modules/codec/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.
Link:	https://trac.videolan.org/vlc/ticket/22240

nist-nvd2

Reference:	CVE-2019-13962
Description:	lavc_CopyPicture in modules/codec/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.
Link:	https://trac.videolan.org/vlc/ticket/22240

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media player Denial of Service Vulnerability

QID:	372568
Category:	Local
Associated CVEs:	CVE-2012-3377
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/04/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

The application is vulnerable to Heap-based buffer overflow in the Ogg_DecodePacket function in the OGG demuxer (modules/demux/ogg.c) in VideoLAN VLC media player before 2.0.2 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted OGG file.

Affected Versions:
VLC media player 2.0.2 and earlier

IMPACT:

Successful exploitation could cause a denial of service (application crash) and possibly execute arbitrary code via a crafted OGG file.

SOLUTION:

The vendor has confirmed the vulnerability and released VLC media player version 2.0.2 to resolve this issue that can be downloaded from here (http://www.videolan.org/vlc/download-windows.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC media player 2.0.2 (http://download.videolan.org/pub/videolan/vlc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media player Buffer Overflow Vulnerability (VideoLAN-SA-1501)

QID:	372641
Category:	Local
Associated CVEs:	CVE-2014-9629
Vendor Reference:	VideoLAN-SA-1501
Bugtraq ID:	-
Service Modified:	07/08/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

The application is vulnerable to Integer overflow in the Encode function in modules/codec/schroedinger.c in VideoLAN VLC media player.

Affected Versions:
VLC media player prior to 2.1.6 and 2.2.x prior to 2.2.1

IMPACT:

Successful exploitation of this vulnerability allows remote attackers to conduct buffer overflow attacks and execute arbitrary code via a crafted length value.

SOLUTION:

The vendor has confirmed the vulnerability and released VLC media player version 2.1.6 , 2.2.1 to resolve this issue that can be downloaded from here (http://www.videolan.org/vlc/download-windows.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VLC media player (http://download.videolan.org/pub/videolan/vlc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VLC Media Player Multiple Vulnerabilities (VideoLAN-SB-VLC-312)

QID:	375203
Category:	Local
Associated CVEs:	CVE-2020-26664
Vendor Reference:	VideoLAN-SB-VLC-312
Bugtraq ID:	-
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is a cross-platform media player.

A remote user could create a specifically crafted file that could trigger some various issues, notably 2 read buffer overflows, and some invalid pointers being dereferenced.

Affected Versions:
VLC media player 3.0.11 and earlier

IMPACT:

This vulnerability could be exploited to change contents or configuration on the system. Additionally this vulnerability can also be used to

cause a denial of service in the form of interruptions in resource availability.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to Security Advisory 3012 (https://www.videolan.org/security/sb-vlc3012.html) to obtain additional details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Security Advisory 3012: wndows (https://www.videolan.org/security/sb-vlc3012.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-26664
Description: A vulnerability in EbmlTypeDispatcher::send in VideoLAN VLC media player 3.0.11 allows attackers to trigger a heap-based buffer overflow via a crafted .mkv file.
Link:
https://gist.githubusercontent.com/henices/db11664dd45b9f322f8514d182aef5ea/raw/d56940c8bf211992bf4f3309a85bb2b69383e511

nist-nvd2

Reference: CVE-2020-26664
Description: A vulnerability in EbmlTypeDispatcher::send in VideoLAN VLC media player 3.0.11 allows attackers to trigger a heap-based buffer overflow via a crafted .mkv file.
Link:
https://gist.githubusercontent.com/henices/db11664dd45b9f322f8514d182aef5ea/raw/d56940c8bf211992bf4f3309a85bb2b69383e511

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC NULL Dereference Vulnerability (VideoLAN-SA-1107)

QID:	375424
Category:	Local
Associated CVEs:	CVE-2011-3333
Vendor Reference:	VideoLAN-SA-1107
Bugtraq ID:	-
Service Modified:	08/16/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is a cross-platform media player.

A remote user could create a specifically crafted file that could trigger some various issues, notably 2 read buffer overflows, and some invalid pointers being dereferenced.

Affected Versions:
VLC Prior to 1.1.11

IMPACT:

On Successful exploitation a malicious third party could trigger either a crash of VLC or an arbitratry code execution with the privileges of the target user.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to Security Advisory VideoLAN-SA-1107 (https://www.videolan.org/security/sa1107.html) to obtain additional details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1107: Windows (https://www.videolan.org/security/sa1107.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 Mozilla Firefox Heap Buffer Overflow Vulnerability (MFSA2023-40)

QID:	378859
Category:	Local
Associated CVEs:	CVE-2023-4863
Vendor Reference:	MFSA2023-40
Bugtraq ID:	-
Service Modified:	09/12/2024

User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Affected Products:
Prior to Firefox 117.0.1

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. you can also refer MFSA2023-40 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2023-40 (https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2023-4863
Description: mistymntncop/CVE-2023-4863 exploit repository
Link: https://github.com/mistymntncop/CVE-2023-4863

Reference: CVE-2023-4863
Description: caoweiquan322/NotEnough exploit repository
Link: https://github.com/caoweiquan322/NotEnough

cisa-kev

Reference: CVE-2023-4863
Description: Google Chromium Heap-Based Buffer Overflow Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2023-4863
Description: Google Chrome Heap buffer overflow in WebP
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2023-4863
Description: The WebP 0day
Link: https://blog.isosceles.com/the-webp-0day/

nist-nvd2

Reference: CVE-2023-4863
Description: Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)
Link: https://news.ycombinator.com/item?id=37478403

Reference: CVE-2023-4863
Description: Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)
Link: https://stackdiary.com/critical-vulnerability-in-webp-codec-cve-2023-4863/

Reference: CVE-2023-4863

Description: Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)
Link: https://sethmlarson.dev/security-developer-in-residence-weekly-report-16

Reference: CVE-2023-4863
Description: Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)
Link: https://blog.isosceles.com/the-webp-0day/

? microsoft-cvrf
Reference: CVE-2023-4863
Description: Chromium: CVE-2023-4863 Heap buffer overflow in WebP
Link: https://api.msrc.microsoft.com/cvrf/2023-Sep?api-version=2020

ASSOCIATED MALWARE:
? ReversingLabs
Malware ID: CVE-2023-4863
Type: Exploit
Platform: Package,Image,Win32,Script,Text,Android,Binary

Malware ID: Hqwar
Type: Dropper
Platform: Android

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

3 Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size Vulnerability (Sweet32)

QID:	378985
Category:	Local
Associated CVEs:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS

protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.
More information can be found at Sweet32 (https://sweet32.info/), Microsoft Windows

TLS changes docs (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server) and

Microsoft Transport Layer Security (TLS) registry settings (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2016-2183
Description: IBM Informix Dynamic Server DLL Injection / Code Execution
Link: https://packetstormsecurity.com/files/142756/IBM-Informix-Dynamic-Server-DLL-Injection-Code-Execution.html

0day.today

Reference: CVE-2016-2183
Description: IBM Informix Dynamic Server / Informix Open Admin Tool - DLL Injection / Remote Code Execution / Hea
Link: https://0day.today/exploit/27866

nist-nvd2

Reference: CVE-2016-2183
Description: The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
Link: https://www.exploit-db.com/exploits/42091/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002 Functions is missing.
TLS_RSA_WITH_3DES_EDE_CBC_SHA

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168 Enabled is missing.

3 VideoLAN VLC Media player Multiple Vulnerabilities (VideoLAN-SB-VLC-3019)

QID:	379007
Category:	Local
Associated CVEs:	CVE-2023-46814
Vendor Reference:	VideoLAN-SB-VLC-3019
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:VLC media player 3.0.18 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to VideoLAN-SB-VLC-3019 (https://www.videolan.org/security/sb-vlc3019.html) to obtain more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3019 (https://www.videolan.org/security/sb-vlc3019.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 VideoLAN VLC Media player Vulnerability fixed in VLC media player (VideoLAN-SB-VLC-3020)

QID:	379008
Category:	Local
Associated CVEs:	CVE-2023-47359, CVE-2023-47360
Vendor Reference:	VideoLAN-SB-VLC-3020
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:VLC media player 3.0.19 and earlier

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target system.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to VideoLAN-SB-VLC-3020 (https://www.videolan.org/security/sb-vlc3020.html) to obtain more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3020 (https://www.videolan.org/security/sb-vlc3020.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference:	CVE-2023-47359
Description:	Videolan VLC prior to version 3.0.20 contains an incorrect offset read that leads to a Heap-Based Buffer Overflow in function GetPacket() and results in a memory corruption.
Link:	https://0xariana.github.io/blog/real_bugs/vlc/mms
Reference:	CVE-2023-47360
Description:	Videolan VLC prior to version 3.0.20 contains an Integer underflow that leads to an incorrect packet length.
Link:	https://0xariana.github.io/blog/real_bugs/vlc/mms

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 Libcurl Denial of Service (DoS) Vulnerability

QID:	380508
Category:	Local
Associated CVEs:	CVE-2024-7264
Vendor Reference:	Curl Security Advisory
Bugtraq ID:	-
Service Modified:	09/20/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the time fraction, leading to a strlen() getting performed on a pointer to a heap buffer area that is not (purposely) null terminated.

Affected Versions:
All Curl versions from 7.32.0 up to and including 8.9.0

IMPACT:

Successful exploitation of the vulnerability may leads to a crash and leading to possible confidentiality and integrity loss.

SOLUTION:

Vendor has released patch addressing the vulnerability. For more information, please refer to the Curl Security Advisory (https://curl.se/docs/CVE-2024-7264.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Curl Security Advisory (https://curl.se/docs/CVE-2024-7264.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference:	CVE-2024-7264
Description:	libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcu
Link:	https://hackerone.com/reports/2629968

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\System32\curl.exe Version is 8.4.0.0
%windir%\SysWOW64\curl.exe Version is 8.4.0.0

2 NetBIOS Name Accessible

QID:	70000
Category:	SMB / NETBIOS

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESKTOP-LN5HE01

 2 Enabled Cached Logon Credential

QID:	90007
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Windows NT may use a cache to store the last interactive logon (i.e. console logon), to provide a safe logon for the host in the event that the Domain Controller goes down. This feature is currently activated on this host.

IMPACT:

Unauthorized users can gain access to this cached information, thereby obtaining sensitive logon information.

SOLUTION:

We recommend that you locate the following Registry key, and then set or create a REG_SZ 'CachedLogonsCount' entry with a '0' value:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Nt\CurrentVersion\Winlogon

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon cachedlogonscount = 10

 2 Default Windows Administrator Account Name Present

QID:	90081
Category:	Windows
Associated CVEs:	CVE-1999-0585
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner probed the LSA, Local Security Authority, for the administrator account's name. The target has the default/out-of-the-box name "Administrator" set.

IMPACT:

Most attackers and malicious scripts assume an administrator account name of "Administrator" on Windows systems. If the target has not changed this name, it will simplify the task of the attacker, for example in bruteforcing the password for the account.

SOLUTION:

Change the administrator account's name to a non-default value.

Please note that if the scanner has been configured to use Windows Authentication and uses the local administrator account (as against a domain-admin account) to scan this target, the scanner will need to be reconfigured to use the new administrator account name instead.

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Administrator

2 Microsoft Windows Explorer AutoPlay Not Disabled

QID:	105170
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/13/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The setting that prevents applications from any drive to be automatically executed is not enabled on the host.

IMPACT:

Exploiting this vulnerability can cause malicious applications to be executed unintentionally at escalated privilege.

SOLUTION:

Disable autoplay from any disk type by setting the value NoDriveTypeAutoRun to 255 under this registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\explorer.exe found
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.

2 Windows Explorer Autoplay Not Disabled for Default User

QID:	105171
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The setting that prevents applications from any drive to be automatically executed when no user is logged in is not enabled on the host.

IMPACT:

An attacker may be able to run an unauthorized application.

SOLUTION:

Make sure that the value NoDriveTypeAutoRun is defined under this registry key:

HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\explorer.exe found
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoAutorun is missing.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.
HKU\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.

 2 VLC Media Player Meta-Information Remote Denial of Service Vulnerability

QID:	118383
Category:	Local
Associated CVEs:	CVE-2010-2937
Vendor Reference:	VideoLAN-SA-1004
Bugtraq ID:	42386
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

VLC media player is a cross-platform media player that can be used to serve streaming data.

VLC fails to perform sufficient input validation when trying to extract some meta-information about input media through ID3v2 tags. In the failure case, VLC attempt dereference an invalid memory address, and a crash will ensure.

In the failure case, VLC will dereference a memory address within the first page of its process virtual memory. In normal conditions, and on most operating systems, this will result in a segmentation fault (a general protection fault on Windows), and the process will terminate abruptly.In most usage scenario, this will only cause user annoyance.

Affected Versions:
VLC media player Versions 1.1.2 down to 0.9.0

IMPACT:

If this vulnerability is successfully exploited, attackers can crash the affected application, denying service to legitimate users, or possibly

execute arbitrary code.

SOLUTION:

The latest patch is available for download fromVLC Web site (http://www.videolan.org/).

Refer to vendor advisory VideoLAN-SA-1004 (http://www.videolan.org/security/sa1004.html) to obtain additional details about the vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SA-1004: Windows (VLC Media Player)
(http://git.videolan.org/?p=vlc/vlc-1.1.git;a=blobdiff;f=modules/meta_engine/taglib.cpp;h=e92714807ce2f23b741d6becb1049b85eb766fea;hp=9ddb26e331c99bf9b96208e7d08cc0e94a6aa698;hb=24918843e57c7962e28fcb01845adce82bed6516;hpb=246a53cdef8f3bd32e93b165806089ae86dfbfa5)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe found
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0
C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

2 Microsoft Windows Snipping Tool Information Disclosure Vulnerability

QID:	378131
Category:	Local
Associated CVEs:	CVE-2023-28303
Vendor Reference:	Microsoft Windows Snipping Tool Studio Advisory
Bugtraq ID:	-
Service Modified:	06/14/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Snipping Tool is a Microsoft Windows screenshot utility, it can take still screenshots of an open window, rectangular areas, a free-form area, or the entire screen.

CVE-2023-28303: Microsoft Windows Snipping Tool is vulnerable to Information Disclosure Vulnerability.

Affected Versions:
Snip and Sketch installed on Windows 10, app versions prior to 10.2008.3001.0
Snipping Tool installed on Windows 11, app versions prior to 11.2302.20.0

Patched Versions:
For Snip and Sketch installed on Windows 10, app versions 10.2008.3001.0 and later contain this update.
For Snipping Tool installed on Windows 11, app versions 11.2302.20.0 and later contain this update.

NOTE:
Only Snip/Sketch in Windows 10 and Snipping Tool in Windows 11 are affected by this vulnerability.

IMPACT:

Successful exploitation may allow an attacker ability to recover parts of the original image if partially overwritten through the use of a special tool.

SOLUTION:

Customers are advised to upgrade latest available version to remediate this vulnerability. For more information please refer to Microsoft Windows Snipping Tool Studio Advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28303).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows Snipping Tool Studio Advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28303)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Version '10.1907.2471.0'

2 Mozilla Firefox Multiple Vulnerabilities (MFSA2024-39)

QID:	380428
Category:	Local
Associated CVEs:	CVE-2024-8386, CVE-2024-8382, CVE-2024-8381, CVE-2024-8387, CVE-2023-6870, CVE-2024-8388, CVE-2024-8384, CVE-2024-8385, CVE-2024-8383, CVE-2024-8389
Vendor Reference:	MFSA2024-39
Bugtraq ID:	-
Service Modified:	09/05/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.

Mozilla Firefox is prone to
CVE-2024-8385: WASM type confusion involving ArrayTypes
CVE-2024-8381: Type confusion when looking up a property name in a "with" block
CVE-2024-8388: Fullscreen notice on Android could be hidden under various panels and OS prompts
CVE-2024-8382: Internal event interfaces were exposed to web content when browser EventHandler listener callbacks ran
CVE-2024-8383: Firefox did not ask before openings news: links in an external application
CVE-2024-8384: Garbage collection could mis-color cross-compartment objects in OOM conditions
CVE-2024-8386: SelectElements could be shown over another site if popups are allowed
CVE-2024-8387: Memory safety bugs fixed in Firefox 130, Firefox ESR 128.2, and Thunderbird 128.2
CVE-2024-8389: Memory safety bugs fixed in Firefox 130

Affected Products:
Prior to Firefox 130

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Upgrade to Firefox 130 to fix vulnerability, you can also refer MFSA2024-39 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2024-39/) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA2024-39 (https://www.mozilla.org/en-US/security/advisories/mfsa2024-39/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 104.0.0.0

Potential Vulnerabilities (5)

4 VideoLAN VLC Media player Vulnerability fixed in VLC media player (VideoLAN-SB-VLC-3021)

QID:	379931
Category:	Local
Associated CVEs:	-
Vendor Reference:	VideoLAN-SB-VLC-3021
Bugtraq ID:	-
Service Modified:	06/19/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

VLC is an open source, cross-platform media player that supports media streaming.

Affected Versions:VLC media player 3.0.20 and earlier

IMPACT:

Successful exploitation of this vulnerability could trigger either a crash of VLC or an arbitrary code execution with the privileges of the target user.

SOLUTION:

The vendor has released updates to resolve this issue. Refer to VideoLAN-SB-VLC-3021 (https://www.videolan.org/security/sb-vlc3021.html) to obtain more information.Workaround:The user should refrain from opening mms streams from untrusted third parties (or disable the VLC browser plugins), until the patch is applied.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VideoLAN-SB-VLC-3021 (https://www.videolan.org/security/sb-vlc3021.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 1.1.0.0

3 Administrator Account's Password Does Not Expire

QID:	90080
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/29/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The scanner probed the Security & Accounts Database (SAM) and found that the target Windows box's Administrator account has a password that does not expire.

IMPACT:

Depending on the site's policy, this may be considered a security vulnerability since it allows attackers an infinite duration to try bruteforcing (guessing over multiple login attempts) the password for the account.

SOLUTION:

Reconfigure the Administrator account's properties to expire the password after a specified duration per the site's policy. Ideally, domain-wide policies should be set on the Domain Controller so that all Windows hosts on the domain comply automatically, and each individual host does not need to be configured.

Note that the Administrator account on the Domain Controller(s) will always have a password that does not expire, since the option check box in the properties dialog box for this account is greyed out. Because of this it is recommended to utilize the following guide for securing Windows domain Administrator accounts: Securing Built-in Administrator Accounts in Active Directory (https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory).

Additional details can be found under QID 45031 "Accounts Enumerated From SAM Database Whose Passwords Do Not Expire."

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Account: Administrator, Password age: -4865 days, Last Password Set Date: (Fri 13 Dec 1901 08:45:52 PM GMT)

 3 Built-in Guest Account Not Renamed at Windows Target System

QID:	105228
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/21/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The built-in Guest account is not renamed at the target Microsoft Windows system.

IMPACT:

Knowing a valid username allows for substantially easier bruteforcing attacks.

SOLUTION:

Rename the Guest account.

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user

account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Guest

2 Global User List Found Using Other QIDS

QID:	45002
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:

These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:

To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	Source Vulnerability (QualysID)
Administrator	45032, 45027, 45031
Guest	90266, 45027, 45031

DefaultAccount	45027, 45031
WDAGUtilityAccount	45027
User	45031

2 Windows User Accounts With Unchanged Passwords

QID:	105236
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The target Microsoft Windows system has some user accounts with passwords which have never changed. This may include any disabled accounts that

you may have.

IMPACT:

N/A

SOLUTION:

Please check if this adheres with your security policy and remove unwanted accounts.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Administrator
DefaultAccount
Guest

Information Gathered (175)

3 Accounts Enumerated From SAM Database Whose Passwords Do Not Expire

QID:	45031
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/30/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Security Accounts Manager holds user and machine account information. The scanner found at least one user or machine account in the SAM database for the target Windows machine whose password does not expire. The accounts are listed in the Result section.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User/Machine Accounts With Passwords That Do Not Expire:
Administrator
DefaultAccount
Guest
User

3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled

QID:	45290
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

The remote host doesn't have Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) disabled.

IMPACT:

attackers can perform a LLMNR poisoning attack to capture usernames and passwords on a local network.

SOLUTION:

Disable the protocol if it's not needed.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient EnableMulticast is missing.

3 NetBIOS Bindings Information

QID:	70004
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be accessible to external networks, and should be firewalled.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Service	NetBIOS Suffix
DESKTOP-LN5HE01	File Server Service	0x20
DESKTOP-LN5HE01	Workstation Service	0x0
WORKGROUP	Domain Name	0x0

 3 NetBIOS Shared Folders

QID:	70030
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/29/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following NetBIOS shared folders have been detected.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Device Name	Comment	Type	Label	Size	Description
ADMIN$	Remote Admin	-2147483648		49 GB	Disk (mounted)
C$	Default share	-2147483648			
IPC$	Remote IPC	-2147483645			

3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines

QID:	90127
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/12/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows Socket (Winsock) parameters at the target are enumerated and compared against the protection levels recommended in TCP/IP hardening guidelines from Microsoft.

IMPACT:

Depending on the services hosted by the target, it may be subject to denial of service attacks.

SOLUTION:

You can secure the TCP/IP stack for Windows Sockets (Winsock) applications such as FTP servers and Web servers. The driver Afd.sys is responsible for
connection attempts to Winsock applications. Afd.sys has been modified in
Windows 2000, Windows 2003, and Windows XP to support large numbers of connections in the half-open state without denying access to legitimate clients. Afd.sys can use dynamic backlog, which is configurable, rather than a static backlog.

You can configure four parameters for the dynamic backlog:

EnableDynamicBacklog: Switches between using a static backlog and a dynamic backlog. By default, this parameter is set to 0, which enables the static backlog. You should enable the dynamic backlog for better security on Winsock.

MinimumDynamicBacklog: Controls the minimum number of free connections
allowed on a listening Winsock endpoint. If the number of free connections
drops below this value, a thread is queued to create additional free
connections. Making this value too large (setting it to a number greater than 100) will degrade the performance of the computer.

MaximumDynamicBacklog: Controls the maximum number of half-open and free connections to Winsock endpoints. If this value is reached, no additional free connections will be made.

DynamicBacklogGrowthDelta: Controls the number of Winsock endpoints in each allocation pool requested by the computer. Setting this value too high can cause system resources to be unnecessarily occupied.

Each of these values must be added to this registry key:
HKLM\System\CurrentControlSet\Services\AFD\Parameters

The recommended levels of protection for these parameters are indicated below.
DynamicBacklogGrowthDelta: 10
EnableDynamicBacklog: 1
MinimumDynamicBacklog: 20
MaximumDynamicBacklog: 20000

Refer to the Microsoft Security Topics document called How To: Harden the TCP/IP Stack (http://msdn.microsoft.com/en-us/library/ff648853.aspx) for

a detailed description of these parameters and other impacts these might have before deploying these settings.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

EnableDynamicBacklog	Recommended:	1	Actual:	Missing
MinimumDynamicBacklog	Recommended:	20	Actual:	Missing
MaximumDynamicBacklog	Recommended:	20, 000	Actual:	Missing
DynamicBacklogGrowthDelta	Recommended:	10	Actual:	Missing

3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines

QID:	90128
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/10/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The target Windows system TCP/IP parameters are enumerated and compared against TCP/IP hardening guidelines from Microsoft.

To help prevent denial of service attacks, you can harden the TCP/IP protocol stack on Windows 2000/2003 and Windows XP computers. You should harden the TCP/IP stack against denial of service attacks, even on internal networks, to prevent denial of service attacks that originate from inside the network as well as on computers attached to public networks.

You can harden the TCP/IP stack on a Windows 2000/2003 or Windows XP computer by customizing these registry values, which are stored in the registry key:
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\

IMPACT:

Depending on the role played by the target, it may be subject to denial of service and other TCP level attacks.

SOLUTION:

EnablePMTUDiscovery: Determines whether path MTU discovery is enabled (1), in which case TCP attempts to discover the largest packet size over the path to a remote host. When path MTU discovery is disabled (0), the path MTU for all TCP connections will be fixed at 576 bytes.

DisableIPSourceRouting: Determines whether a computer allows clients to predetermine the route that packets take to their destination. When this value is set to 2, the computer will disable source routing for IP packets.

NoNameReleaseOnDemand: Determines whether the computer will release its NetBIOS name if requested by another computer or a malicious packet attempting to hijack the computer's NetBIOS name. This is configured under HKLM\System\CurrentControlSet\Services\Netbt\Parameters

PerformRouterDiscovery: Determines whether the computer performs router discovery on this interface. Router discovery solicits router information from the network and adds the information retrieved to the route table. Setting this value to 0 will prevent the interface from performing router discovery.

EnableDeadGWDetect: Determines whether the computer will attempt to detect dead gateways. When dead gateway detection is enabled (by setting this value to 1), TCP might ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways are defined in the TCP/IP configuration dialog box in the Network Control Panel for each adapter. When you leave this setting enabled, it's possible for an attacker to redirect the server to a gateway of his choosing.

EnableICMPRedirect: When ICMP redirects are disabled (by setting the value to 0), attackers cannot carry out attacks that require a host to redirect the ICMP-based attack to a third party.

SynAttackProtect: Enables SYN flood protection in Windows 2000 and Windows XP. You can set this value to 0, 1, or 2. The default setting 0 provides no protection. Setting the value to 1 will activate SYN/ACK protection contained in the TCPMaxPortsExhausted, TCPMaxHalfOpen, and TCPMaxHalfOpenRetried values. Setting the value to 2 will protect against SYN/ACK attacks by more aggressively timing out open and half-open connections. For Windows 2003, the recommended value is 1.

TCPMaxConnectResponseRetransmissions: Determines how many times TCP retransmits an unanswered SYN/ACK message. TCP retransmits acknowledgments until the number of retransmissions specified by this value is reached.

TCPMaxHalfOpen: Determines how many connections the server can maintain in the half-open state before TCP/IP initiates SYN flooding attack protection. This entry is used only when SYN flooding attack protection is enabled on this server, that is when the value of the SynAttackProtect entry is 1 or 2 and the value of the TCPMaxConnectResponseRetransmissions entry is at least 2.

TCPMaxHalfOpenRetired: Determines how many connections the server can maintain in the half open state even after a connection request has been retransmitted. If the number of connections exceeds the value of this entry, TCP/IP initiates SYN flooding attack protection. This entry is used only when SYN flooding attack protection is enabled on this server, that is when the value of the SynAttackProtect entry is 1 and the value of the TCPMaxConnectResponseRetransmissions entry is at least 2.

Refer to the Microsoft Security Topics document called How To: Harden the TCP/IP Stack (http://msdn.microsoft.com/en-us/library/ff648853.aspx) for a detailed description of these parameters and other impacts these might have before deploying these settings.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

EnableICMPRedirect	Recommended:	0	Actual:	1
SynAttackProtect	Recommended:	2	Actual:	Missing
TCPMaxConnectResponseRetransmissions	Recommended:	2	Actual:	Missing
TCPMaxHalfOpen	Recommended:	500	Actual:	Missing
TCPMaxHalfOpenRetried	Recommended:	400	Actual:	Missing
TCPMaxPortsExhausted	Recommended:	5	Actual:	Missing
TCPMaxDataRetransmissions	Recommended:	2	Actual:	Missing
EnableDeadGWDetect	Recommended:	0	Actual:	Missing
EnablePMTUDiscovery	Recommended:	0	Actual:	Missing
DisableIPSourceRouting	Recommended:	1	Actual:	Missing
NoNameReleaseOnDemand	Recommended:	1	Actual:	Missing
PerformRouterDiscovery	Recommended:	0	Actual:	Missing

3 BHOs Detected

QID:	90139
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/20/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A Browser Helper Object (BHO) is a special type of add-in for Microsoft Internet Explorer (IE). A BHO tightly integrates with IE to customize and control the browser application. When IE starts, it scans the registry to create BHOs. Created BHOs have access to all the events and properties of the current browsing session. BHOs can be manually searched using "regedit.exe". For example, Adobe Acrobat installs a BHO and adds it to the registry as described below.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}

where {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} is the UUID of BHO, and InprocServer32 in HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}\InprocServer32 specifies the file path of the BHO. In this example, it is "C:\Program Files\Adobe\Acrobat 5.0\Reader\ActiveX\AcroIEHelper.ocx". Your system might have different path.

The following Browser Helper Objects have been found on your system.

IMPACT:

A maliciously designed BHO, probably installed by Trojans, could potentially snatch data from your online session, including your user name and passwords entered into forms on Web pages, and send anywhere.

SOLUTION:

You can manually delete registry entries to disable unwanted BHOs, but this might create problems. It is highly recommended to use your antivirus software and tools such as BHOcop.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Browser Helper Objects
{1FD49718-1D00-4B19-AF5F-070AF6D5D54C} C:\Program Files (x86)\Microsoft\Edge\Application\129.0.2792.52\BHO\ie_to_edge_bho_64.dll
Browser Helper Objects
{1FD49718-1D00-4B19-AF5F-070AF6D5D54C} C:\Program Files (x86)\Microsoft\Edge\Application\129.0.2792.52\BHO\ie_to_edge_bho_64.dll

3 Administrator Group Members Enumerated

QID:	105231
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/04/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Members of the built-in Administrator Group are enumerated from the target Microsoft Windows system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Administrators {sid="S-1-5-21-4268673589-654920014-3518733957-500", name="DESKTOP-LN5HE01\\Administrator"}
Administrators {sid="S-1-5-21-4268673589-654920014-3518733957-1001", name="DESKTOP-LN5HE01\\User"}

3 SAMR Pipe Permissions Enumerated

QID:	105237
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The account permissions for the SAMR pipe are enumerated from the target Microsoft Windows system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

\SAMR Everyone 0 access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
\SAMR AnonymousLogon 7 access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
\SAMR APPLICATION PACKAGE AUTHORITY\Your Windows credentials 8 access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
\SAMR Administrators 544 access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data

3 Antivirus Product Detected on Windows Host

QID:	105327
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/10/2024
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

One or more of the following Windows Antivirus products were detected on the host:

AVG Antivirus

CA eTrust Antivirus

F-Secure Antivirus

Kaspersky Antivirus

McAfee Antivirus

Network Associates Antivirus

Sophos Antivirus Scanner

Symantec Norton Antivirus Corporate Edition

Symantec Norton Antivirus Personal Edition

Symantec Endpoint Protection

TrendMicro Antivirus

ESET Antivirus Scanner

Microsoft Windows Defender

Clam Antivirus

Lumension EMSS

Microsoft System Center Endpoint Protection

Cylance Antivirus

Crowdstrike Anti virus

Cisco AMP(Advanced Malware Protection)

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows Defender\Signature Updates exists
WinDefend = RUNNING
Windows Defender Installed

 3 Sticky Key's Enabled on System

QID:	124403
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/15/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Sticky Keys is a Windows Ease of Access feature that allows users to use keyboard shortcuts or type capital letters without need of pressing multiple keys.

A privilege elevation exploit has been reported with Sticky Keys, which can be exploited by a local privileged user or an attacker with physical access to gain System access of the machine, by replacing the sethc.exe (Sticky Key executable) with cmd.exe, which can be accessed later on at the login screen by pressing shift key multiple times.

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to obtain elevated access to the system.

SOLUTION:

Microsoft has not confirmed this as a vulnerability and will not be providing any patch.

Workaround:
Administrators is advised to disable

Sticky Keys for all user

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKU\.DEFAULT\Control Panel\Accessibility\StickyKeys Flags = 510

 3 RPC Portmapper Information

QID:	125001
Category:	Forensics
Associated CVEs:	CVE-1999-0632
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The result section shows the information received by making an RPC call to the portmapper on the target host. It shows the list of all registered RPC programs.

IMPACT:

N/A

SOLUTION:

Check to be sure that the information reported adheres to your security policy.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

RPC detected on UDP port 138.
RPC detected on UDP port 500.
RPC detected on UDP port 1900.

2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 10 Pro 64 bit Edition Version 22H2	Windows Registry	
Windows 2016/2019/10	NTLMSSP	
Windows 10	TCP/IP Fingerprint	U7119:135
cpe:/o:microsoft:windows_10:22h2::x64:	CPE	

2 Windows Effective Password Policy Information Gathering Via SAM Database

QID:	45026
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/29/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This check probes the SAM database on the target host for password policy information. Information gathered is:

Minimum Password Age in Days
Maximum Password Age in Days
Minimum Password Length in Characters
Password History (Number of old passwords remembered)

The policy is the effective policy, which is a combination of the local policy settings (if any) and the domain-wide policy settings made on the Domain Controller(s) for the domain.

This probe requires authentication to be successful.

IMPACT:

This password policy information may be used for auditing a Windows-based network for password policy compliance of its nodes. An attacker with a working account can use it to query the network and obtain information.

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: DS5.4 User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

Type: GLBA
Section: N/A
Description: Ensure the confidentiality and protection of passwords through secure password creation and distribution mechanisms.

Type: HIPAA
Section: 164.308(a)(5)(ii)(D)
Description: Password management
Procedures for creating, changing, and safeguarding passwords.

Type: SOX
Section: N/A
Description: User Access Management
Granting resource access, user ID and password requirements, individual accountability, limited utilization of native administrative IDs, non-employee user ID expiration, reporting employee and contractor status changes.
Operating System Access Control
Password enforcement, logon information, password display and printing, required password changes, vendor default passwords, security changes after system compromise, systems software utility usage, automatic log off.
Password Management
Procedures exist that ensure the confidentiality and protection of passwords through secure password creation and distribution mechanisms, the enforcement and adherence to acceptable password standards, and the regular changing of passwords.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Effective Password Policy:

Mininum Password Length - 0 (Not defined/Infinite).
Password History Length - 0 (Not defined/Infinite).
Minimum Password Age - 0 (Not defined/Infinite).
Maximum Password Age - 42 Days.
Password Complexity - Not Set.
Store Password Using Reversible Encryption - Not Set.

 2 Windows Domain Effective Account Lockout Policy Information Gathered Via SAM Database

QID:	45028
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/30/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Security and Accounts Manager (SAM) Database of any Windows host participating in a Windows Domain has information about the account lockout policy set on that system. Such information was gathered from the target and is shown in the Results section below.

It should be noted that if the Domain Controller/Active Directory on this domain enforces a policy as well, the Domain Controller policy will override the local policies (if any) of each host. Further, it takes up to a couple of minutes for changes on the Domain Controller policy to be propogated to all the individual hosts on that domain.

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

Type: GLBA
Section: N/A
Description: Ensure that accounts are locked after unsuccessful login attempts.

Type: HIPAA
Section: 164.312(a)(1)
Description: Standard: Access Control
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access

only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).

Type: SOX
Section: N/A
Description: Ensure that accounts are locked after unsuccessful login attempts and that failed login attempts are logged.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Effective Account Lockout Policy:

Maximum Failed Logon Attempts Before Lockout - 10 Attempts.
Lockout Logon-Attempts-Counter Duration - 10 Minutes.
Lockout Duration - 10 Minutes.

 2 Administrator Account's Real Name Found From LSA Enumeration

QID:	45032
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/04/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

LSA (Local Security Authority Database) is a protected subsystem that authenticates and logs users onto the local system.

Windows systems by default have the administrator account's name configured as "Administrator". This can very easily be changed to a non-default value (like root, for example) to harden security against password bruteforcing.

LSA, internally, refers to user accounts by what are called RIDs (Relative IDs) instead of the friendlier names (like "Administrator") used only for GUI and display purposes. The administrator account on any Windows system always has a RID of 500, even if the name has been changed.

The scanner probed the LSA for the name that maps to the RID of 500, which is the administrator account name, changed or unchanged. The name is listed in the Result section below.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Administrator

2 Microsoft .Net Framework Installed on Target Host

QID:	45178
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Microsoft .NET Framework
Bugtraq ID:	-
Service Modified:	01/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft .NET Framework is a software framework for computers running Microsoft Windows operating systems.

Microsoft .NET Framework is installed on target host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Net Framework	Version	Release	Service Pack	Key
.Net Framework 4.x Client Installation x64	4.8.04084	528372 4.8	-	HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Client
.Net Framework 4.x Full Installation x64	4.8.04084	528372 4.8	-	HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
.Net Framework 4.x Client Installation x86	4.8.04084	528372 4.8	-	HKLM\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client
.Net Framework 4.x Full Installation x86	4.8.04084	528372 4.8	-	HKLM\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full

2 Mozilla Firefox Installed Extensions

QID:	45253
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/17/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Mozilla Firefox is a Web browser developed and released by Mozilla. Extensions are small software programs that can modify and enhance the functionality of the Firefox browser. The result section lists the installed Firefox extensions.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Firefox Extension Location	Name	Version
"C:\\Program Files (x86)\\Mozilla Firefox\\browser\\features\\doh-rollout@mozilla.org.xpi"	DoH Roll-Out	2.0.0
"C:\\Program Files (x86)\\Mozilla Firefox\\browser\\features\\pictureinpicture@mozilla.org.xpi"	Picture-In-Picture	1.0.0
"C:\\Program Files (x86)\\Mozilla Firefox\\browser\\features\\screenshots@mozilla.org.xpi"	Firefox Screenshots	39.0.1
"C:\\Program Files (x86)\\Mozilla Firefox\\browser\\features\\webcompat-reporter@mozilla.org.xpi"	WebCompat Reporter	1.5.0
"C:\\Program Files (x86)\\Mozilla Firefox\\browser\\features\\webcompat@mozilla.org.xpi"	Web Compatibility Interventions	104.6.0

2 Administrator Group Members Enumerated Using SID

QID:	45302
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/04/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Members of the built-in Administrator Group are enumerated from the target Microsoft Windows system using its well-known SID.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

S-1-5-32-544 Administrators {siduse="User", sid="S-1-5-21-4268673589-654920014-3518733957-500", name="DESKTOP-LN5HE01\\Administrator"}
S-1-5-32-544 Administrators {siduse="User", sid="S-1-5-21-4268673589-654920014-3518733957-1001", name="DESKTOP-LN5HE01\\User"}

 2 Model Information from Devices

QID:	45304
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/01/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Hardware Model Information is an Important data required while we Discover the Devices.

Adding Hardware Model/Product information will be provide Better Visibility of the Devices Across the IT Infrastructure.

Authenticate if required against a Device and Run Commands to Get/Fetch the Model Information of a Device.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\SystemInformation		
SystemProductName	=	VirtualBox
HKLM\SOFTWARE\Microsoft\Cryptography		
MachineGuid	=	2b28a13d-dc5f-4942-9804-1070cc52945f

 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0				\PIPE\epmapper
DCE Remote Management	1.0				\PIPE\epmapper
DCOM OXID Resolver	0.0				\PIPE\epmapper
DCOM Remote Activation	0.0				\PIPE\epmapper
DCOM System Activator	0.0				\PIPE\epmapper
Microsoft Event Log Service	0.0				\PIPE\eventlog
Microsoft Local Security Architecture	0.0				\PIPE\lsarpc
Microsoft Registry	1.0				\PIPE\winreg
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc
Microsoft Security Account Manager	1.0	49664			\PIPE\samr, \pipe\lsass
Microsoft Server Service	3.0				\PIPE\srvsvc
Microsoft Service Control Service	2.0	49669			\PIPE\svcctl
Microsoft Spool Subsystem	1.0	49668			\PIPE\spoolss
Microsoft Task Scheduler	1.0				\PIPE\atsvc
Microsoft Workstation Service	1.0				\PIPE\wkssvc
WinHttp Auto-Proxy Service	5.1	49666			\pipe\eventlog
Microsoft Spool Subsystem	1.0				\PIPE\SPOOLSS
Ngc Pop Key Service	1.0	49664			\pipe\lsass
KeyIso	2.0	49664			\pipe\lsass
(Unknown Service)	1.0	49665			\PIPE\InitShutdown
(Unknown Service)	1.0				\PIPE\InitShutdown
(Unknown Service)	1.0				\pipe\LSM_API_service
(Unknown Service)	1.0	49667			\pipe\LSM_API_service, \PIPE\srvsvc, \PIPE\atsvc
(Unknown Service)	0.0				\pipe\LSM_API_service
(Unknown Service)	2.0				\pipe\LSM_API_service
Impl friendly name	1.0	49667			\PIPE\srvsvc, \PIPE\atsvc
IKE/Authip API	1.0	49667			\PIPE\srvsvc, \PIPE\atsvc
AppInfo	1.0	49667			\PIPE\srvsvc, \PIPE\atsvc

IdSegSrv service	1.0	49667	\PIPE\atsvc
Adh APIs	1.0	49667	\PIPE\atsvc
XactSrv service	1.0	49667	\PIPE\atsvc
Proxy Manager client server endpoint	1.0	49667	\PIPE\atsvc
Proxy Manager provider server endpoint	1.0	49667	\PIPE\atsvc
IP Transition Configuration endpoint	1.0	49667	\PIPE\atsvc
(Unknown Service)	1.0	49667	\PIPE\atsvc
(Unknown Service)	2.0		\PIPE\atsvc
UserMgrCli	1.0		\PIPE\atsvc
DHCPv6 Client LRPC Endpoint	1.0	49666	\pipe\eventlog
DHCP Client LRPC Endpoint	1.0	49666	\pipe\eventlog
Event log TCPIP	1.0	49666	\pipe\eventlog
Remote Fw APIs	1.0	50464	
(Unknown Service)	1.0	49668	
DfsDs service	1.0		\PIPE\wkssvc
(Unknown Service)	1.0		\pipe\trkwks
PcaSvc	1.0		\pipe\trkwks
(Unknown Service)	0.0		\pipe\trkwks

2 Installed Applications Enumerated From Windows Installer

QID:	90235
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The installed applications at the Windows host are listed. This test obtains this list by querying the registry keys corresponding to the Installer Database.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Display Name	Display Version	Install Date	Publisher	Language	Install Path	Uninstall String
Mozilla Maintenance Service	104.0		Mozilla			"C:\Program Files (x86)\Mozilla Maintenance Service\uninstall.exe"

	7.1.0.164728		Oracle and/or its affiliates		C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
Microsoft Edge	129.0.2792.52	20240923	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application	"C:\Program Files (x86)\Microsoft\Edge\Application\129.0.2792.52\Installer\setup.exe" --uninstall --msedge --channel=stable --system-level --verbose-logging
Microsoft Edge Update	1.3.195.19				
Microsoft Edge WebView2 Runtime	128.0.2739.79	20240923	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application	"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\128.0.2739.79\Installer\setup.exe" --uninstall --msedgewebview --system-level --verbose-logging
Mozilla Firefox (x86 en-US)	104.0		Mozilla	C:\Program Files (x86)\Mozilla Firefox	"C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe"
VLC media player 1.1.1	1.1.1		VideoLAN	C:\Program Files (x86)\VideoLAN\VLC	C:\Program Files (x86)\VideoLAN\VLC\uninstall.exe

2 Real Name of Built-in Guest Account Enumerated

QID:	90266
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/30/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft best practices documents recommend renaming the built-in Guest account. This test enumerates the actual name of the built-in Guest account.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Guest

2 Microsoft XML parser (MSXML) Versions Detected

QID:	91228
Category:	Windows
Associated CVEs:	-
Vendor Reference:	KB269238
Bugtraq ID:	-
Service Modified:	11/16/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft XML Core Services (MSXML) is a set of services that allow applications written in JScript, VBScript, and Microsoft development tools to build Windows-native XML-based applications.

Different versions of MSXML are included with various Microsoft products, such as Microsoft Windows, Microsoft Internet Explorer, Microsoft Office, and Microsoft SQL Server. MSXML is also updated when you install software updates for various Microsoft products. The MSXML parser is included in the Msxml.dll file, the Msxml2.dll file, the Msxml3.dll file, the Msxml4.dll file, the Msxml5.dll file, the Msxml6.dll file, and one or more resource files.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft XML parser (MSXML) v3 8.110.19041.3636
Microsoft XML parser (MSXML) v6 6.30.19041.3636
Microsoft XML parser (MSXML) v3 8.110.19041.3636
Microsoft XML parser (MSXML) v6 6.30.19041.3636

2 Microsoft Windows Users With Privilege - Assign Primary Token Privilege

QID:	105099
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeAssignPrimaryTokenPrivilege setting at the host is enumerated. By default Local Service and Network Service have this privilege. Local System has the privilege inherently.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT AUTHORITY\NETWORK SERVICE

NT AUTHORITY\LOCAL SERVICE

 2 Microsoft Windows Users With Privilege - Audit Privilege

QID:	105100
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeAuditPrivilege setting at the host is enumerated. By default Local Service and Network Service accounts have this privilege. Local System has the privilege inherently.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT AUTHORITY\NETWORK SERVICE

NT AUTHORITY\LOCAL SERVICE

2 Microsoft Windows Users With Privilege - Backup Files and Directories

QID:	105101
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeBackupPrivilege setting allows the user to circumvent file and directory permissions to back up the system. The privilege is selected only when an application attempts access by using the NTFS backup application programming interface API. Otherwise, normal file and directory permissions apply. By default administrators and backup operators have access.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Change Notify

QID:	105102
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Allows a user to passthrough folders to which the user otherwise has no access while navigating an object path in the NTFS file system or in the registry. This privilege does not allow the user to list the contents of a folder; it allows the user only to traverse its directories. By default administrators, backup operators, power users, users who have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators
Builtin\Users
Builtin\Administrators
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\LOCAL SERVICE
Everyone

2 Microsoft Windows Users With Privilege - Create Global Objects

QID:	105103
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeCreateGlobalPrivilege setting at the host is enumerated. This privilege is required to create named file mapping objects in the global namespace during Terminal Services sessions. This privilege is enabled by default for administrators, services and the Local System account.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.9
Description: Malicious Software Prevention, Detection and Correction
Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT AUTHORITY\SERVICE
Builtin\Administrators
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\LOCAL SERVICE

 2 Microsoft Windows Users With Privilege - Create Page File

QID:	105104
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeCreatePagefile privilege setting at the host is enumerated. This allows users to create and change the size of a page file. This is done by specifying a page file size for a particular drive in the "performance options" box on the Advanced tab of System Properties. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Debug Applications

QID:	105107
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeDebugPrivilege setting at the host is enumerated. This allows a user to attach a debugger to any process. This privilege provides access to sensitive system components and allows for the creation of operating system components.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Impersonate

QID:	105109
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeImpersonatePrivilege setting at the host is enumerated. This allows a user to impersonate a client after authentication.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT AUTHORITY\SERVICE
Builtin\Administrators
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\LOCAL SERVICE

 2 Microsoft Windows Users With Privilege - Increase Base Priority

QID:	105110
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeIncreaseBasePriorityPrivilege setting at the host is enumerated. This allows a user to increase the base priority class of a process. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Window Manager\Window Manager Group

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Increase Quota

QID:	105111
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeIncreaseQuotaPrivilege setting at the host is enumerated. This allows a process that has access to a second process to increase the processor quota assigned to the second process. By default administrators, Local Service and Network Service have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

NT AUTHORITY\NETWORK SERVICE

NT AUTHORITY\LOCAL SERVICE

2 Microsoft Windows Users With Privilege - Load Drivers

QID:	105112
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeLoadDriverPrivilege setting at the host is enumerated. This allows a user to load or unload a driver. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Profile Single Process

QID:	105114
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Allows a user to sample the performance of an application process. By default administrators and power users are vulnerable.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Remote Shutdown

QID:	105115
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeRemoteShutdownPrevilage setting at the host is enumerated. This allows users to shutdown a system from a remote system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Restore

QID:	105116
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeRestorePrivilege setting at the host is enumerated. This allows a user to circumvent file and directory permissions when restoring backed-up files and directories, and to set any valid security principal as the owner of an object. By default administrators and backup

operators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Change Security Attributes

QID:	105117
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/21/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeSecurityPrivilege setting at the host is enumerated. This allows users to specify object access auditing options for individual resources such as files, active directory objects, and registry keys. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Shutdown

QID:	105118
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeShutdownPrivilege setting at the host is enumerated. This allows a user to shutdown a local computer. By default administrators, backup operators, power users and users have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators

Builtin\Users

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Manage Volumes

QID:	105119
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeManageVolumePrivilege setting at the host is enumerated. This allows a non-administrative or remote user to manage volumes or disks. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privileges - Profile System

QID:	105122
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeSystemProfilePrivilege setting at the host is enumerated. This allows a user to sample the performance of system processes. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT SERVICE\WdiServiceHost

Builtin\Administrators

2 Microsoft Windows Users With Privileges - Modify System Time

QID:	105123
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/22/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeSystemTimePrivilege setting at the host is enumerated. This allows a user to adjust the time on the computer's internal clock. By default administrators and power users have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

NT AUTHORITY\LOCAL SERVICE

2 Microsoft Windows Users With Privileges - Take Object Ownership

QID:	105124
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The SeTakeOwnershipPrivilege setting at the host is enumerated. This allows a user to take ownership of any securable object in the system including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes and threads. By default administrators have this privilege.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Administrators

2 Microsoft Windows Users With Privilege - Undock Privilege

QID:	105126
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The SeUndockPrivilege setting at the host is enumerated. This allows the user of a portable computer to undock the computer by checking Eject PC at the start menu.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Users

Builtin\Administrators

2 Microsoft Windows Users With Rights - Logon as a Batch

QID:	105156
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts with batch logon rights are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Performance Log Users

Builtin\Backup Operators

Builtin\Administrators

2 Microsoft Windows Users With Rights - Interactive Logon

QID:	105157
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts with interactive logon rights are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators
Builtin\Users
Builtin\Administrators
DESKTOP-LN5HE01\Guest

2 Microsoft Windows Users With Rights - Network Logon

QID:	105158
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts with network logon rights are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Builtin\Backup Operators

Builtin\Users

Builtin\Administrators

Everyone

2 Microsoft Windows Users With Rights - Logon as a Service

QID:	105159
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts with service logon rights are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NT SERVICE\ALL SERVICES

2 Microsoft Windows Users With Rights Denied - Interactive Logon

QID:	105161
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts for which the interactive logon is explicitly denied are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESKTOP-LN5HE01\Guest

2 Microsoft Windows Users With Rights Denied - Network Logon

QID:	105162
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The accounts for which network logon is explicitly denied are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESKTOP-LN5HE01\Guest

2 Windows Auto Reboot After Blue Screen Not Disabled

QID:	105172
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Auto Reboot after blue screen is enabled on the host. It can be used for activating planted applications that require reboot by causing a system error.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\CrashControl AutoReboot = 1

2 Microsoft Windows Win32 Services Security Analysis

QID:	105183
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This test enumerates the security permissions of non-disabled services on the target Windows system.

IMPACT:

Unauthorized users might be able to control critical system components and modify their configuration.

SOLUTION:

Make sure only administrative users have access to the control of system services.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Access	ACL1	ACL2	ACL3
Appinfo	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Appinfo	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Appinfo	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Appinfo	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Appinfo	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Appinfo	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Appinfo	Access Allowed for Administrators	stop-service	pause-continue-service	-
Appinfo	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Appinfo	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
Appinfo	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
Appinfo	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Appinfo	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Appinfo	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
AudioEndpointBuilder	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
AudioEndpointBuilder	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
AudioEndpointBuilder	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
AudioEndpointBuilder	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
AudioEndpointBuilder	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
AudioEndpointBuilder	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
AudioEndpointBuilder	Access Allowed for Administrators	stop-service	pause-continue-service	-
AudioEndpointBuilder	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
AudioEndpointBuilder	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
AudioEndpointBuilder	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
AudioEndpointBuilder	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Audiosrv	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Audiosrv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Audiosrv	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Audiosrv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac

Audiosrv	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Audiosrv	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
Audiosrv	Access Allowed for Administrators	stop-service	pause-continue-service	-
Audiosrv	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Audiosrv	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Audiosrv	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Audiosrv	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Audiosrv	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
Audiosrv	Access Allowed for S-1-15-2-1	enumerate-service-dependents	nterrogate-service	-
Audiosrv	Access Allowed for S-1-15-3-1024-1692970155-4054893335-1857140913362601943-3526593181159816984-2199008581497492991	standard-read	query-service-config	query-service-status
Audiosrv	Access Allowed for S-1-15-3-1024-1692970155-4054893335-1857140913362601943-3526593181159816984-2199008581497492991	enumerate-service-dependents	nterrogate-service	-
BFE	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
BFE	Access Allowed for Authenticated_Users	nterrogate-service	-	-
BFE	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
BFE	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
BFE	Access Allowed for Local_System	enumerate-service-dependents	start-service	nterrogate-service
BFE	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
BFE	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-dependents
BFE	Access Allowed for Administrators	start-service	nterrogate-service	-
BFE	Access Allowed for Users	query-service-config	query-service-status	nterrogate-service
BrokerInfrastructure	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
BrokerInfrastructure	Access Allowed for Authenticated_Users	nterrogate-service	-	-
BrokerInfrastructure	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
BrokerInfrastructure	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
BrokerInfrastructure	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
BrokerInfrastructure	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
BrokerInfrastructure	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
BrokerInfrastructure	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-dependents
BrokerInfrastructure	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
BrokerInfrastructure	Access Allowed for Administrators	nterrogate-service	-	-
BrokerInfrastructure	Access Allowed for Users	query-service-config	query-service-status	start-service
BrokerInfrastructure	Access Allowed for Users	nterrogate-service	-	-
BthAvctpSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status

BthAvctpSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
BthAvctpSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
BthAvctpSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
BthAvctpSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
BthAvctpSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
BthAvctpSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
BthAvctpSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
BthAvctpSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
BthAvctpSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
BthAvctpSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CDPSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CDPSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CDPSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CDPSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CDPSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CDPSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CDPSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
CDPSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CDPSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CDPSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CDPSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CDPSvc	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
CoreMessagingRegistrar	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CoreMessagingRegistrar	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CoreMessagingRegistrar	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CoreMessagingRegistrar	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
CoreMessagingRegistrar	Access Allowed for Administrators	enumerate-service-de pendents	start-service	stop-service
CoreMessagingRegistrar	Access Allowed for Administrators	pause-continue-service	nterrogate-service	service-user-defined-control
CoreMessagingRegistrar	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CoreMessagingRegistrar	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
CoreMessagingRegistrar	Access Allowed for Service_Logon	service-user-defined-control	-	-
CoreMessagingRegistrar	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CoreMessagingRegistrar	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
CoreMessagingRegistrar	Access Allowed for Interactive_Logon	service-user-defined-control	-	-

CoreMessagingRegistrar	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
CoreMessagingRegistrar	Access Allowed for S-1-15-2-1	enumerate-service-dependents	start-service	nterrogate-service
CoreMessagingRegistrar	Access Allowed for S-1-15-2-1	service-user-defined-control	-	-
CryptSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
CryptSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CryptSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CryptSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CryptSvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
CryptSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
CryptSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
CryptSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
CryptSvc	Access Allowed for System_Operators	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for System_Operators	enumerate-service-dependents	start-service	stop-service
CryptSvc	Access Allowed for System_Operators	pause-continue-service	nterrogate-service	service-user-defined-control
CryptSvc	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for S-1-15-2-1	enumerate-service-dependents	nterrogate-service	-
CryptSvc	Access Allowed for S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334	standard-read	query-service-config	query-service-status
CryptSvc	Access Allowed for S-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-765664414-2751773334	enumerate-service-dependents	nterrogate-service	-
DcomLaunch	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
DcomLaunch	Access Allowed for Authenticated_Users	nterrogate-service	-	-
DcomLaunch	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
DcomLaunch	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
DcomLaunch	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
DcomLaunch	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
DcomLaunch	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DcomLaunch	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-dependents
DcomLaunch	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
DcomLaunch	Access Allowed for Administrators	nterrogate-service	-	-
DcomLaunch	Access Allowed for Users	query-service-config	query-service-status	nterrogate-service
DeviceAssociationService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status

DeviceAssociationService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
DeviceAssociationService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DeviceAssociationService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DeviceAssociationService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
DeviceAssociationService	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
DeviceAssociationService	Access Allowed for Administrators	stop-service	pause-continue-service	-
DeviceAssociationService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DeviceAssociationService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
DeviceAssociationService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DeviceAssociationService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Dhcp	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
Dhcp	Access Allowed for Authenticated_Users	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Dhcp	Access Allowed for Network_Configuration_ Operators	standard-read	query-service-config	query-service-status
Dhcp	Access Allowed for Network_Configuration_ Operators	enumerate-service-de pendents	start-service	stop-service
Dhcp	Access Allowed for Network_Configuration_ Operators	pause-continue-service	nterrogate-service	service-user-defined-control
Dhcp	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Dhcp	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Dhcp	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Dhcp	Access Allowed for Administrators	stop-service	pause-continue-service	-
Dhcp	Access Allowed for Local	standard-read	query-service-config	query-service-status
Dhcp	Access Allowed for Local	enumerate-service-de pendents	start-service	nterrogate-service
Dhcp	Access Allowed for Local	service-user-defined-control	-	-
Dhcp	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Dhcp	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Dhcp	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DiagTrack	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
DiagTrack	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
DiagTrack	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DiagTrack	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DiagTrack	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
DiagTrack	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
DiagTrack	Access Allowed for Administrators	stop-service	pause-continue-service	-
DiagTrack	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DiagTrack	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

DiagTrack	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DiagTrack	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
DispBrokerDesktopSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
DispBrokerDesktopSvc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
DispBrokerDesktopSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DispBrokerDesktopSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DispBrokerDesktopSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
DispBrokerDesktopSvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
DispBrokerDesktopSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
DispBrokerDesktopSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DispBrokerDesktopSvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
DispBrokerDesktopSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DispBrokerDesktopSvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Dnscache	Access Allowed for Users	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Users	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Administrators	enumerate-service-dependents	start-service	pause-continue-service
Dnscache	Access Allowed for Administrators	nterrogate-service	-	-
Dnscache	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Local_System	enumerate-service-dependents	start-service	pause-continue-service
Dnscache	Access Allowed for Local_System	nterrogate-service	-	-
Dnscache	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for Network_Service	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Network_Service	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for Local_Service	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Local_Service	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for Network_Configuration_Operators	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for Network_Configuration_Operators	enumerate-service-dependents	start-service	pause-continue-service
Dnscache	Access Allowed for Network_Configuration_Operators	nterrogate-service	-	-
Dnscache	Access Allowed for S-1-5-80-2940520708-3855866260-481812779-327648279-1710889582	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for S-1-5-80-2940520708-3855866260-481812779-327648279-1710889582	enumerate-service-dependents	pause-continue-service	nterrogate-service

Dnscache	Access Allowed for S-1-5-80-2940520708-3855866260-481812779-327648279-1710889582	service-user-defined-control	-	-
Dnscache	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for S-1-15-2-1	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for S-1-15-3-1	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for S-1-15-3-1	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for S-1-15-3-2	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for S-1-15-3-2	enumerate-service-dependents	start-service	nterrogate-service
Dnscache	Access Allowed for S-1-15-3-3	standard-read	query-service-config	query-service-status
Dnscache	Access Allowed for S-1-15-3-3	enumerate-service-dependents	start-service	nterrogate-service
DPS	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
DPS	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
DPS	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
DPS	Access Allowed for Local_System	stop-service	pause-continue-service	-
DPS	Access Allowed for Administrators	standard-read	query-service-config	change-service-config
DPS	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
DPS	Access Allowed for Administrators	stop-service	pause-continue-service	nterrogate-service
DPS	Access Allowed for Administrators	service-user-defined-control	-	-
DPS	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DPS	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
DPS	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DPS	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
DusmSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
DusmSvc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
DusmSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DusmSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DusmSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
DusmSvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
DusmSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
DusmSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DusmSvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
DusmSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DusmSvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
EventLog	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
EventLog	Access Allowed for Authenticated_Users	enumerate-service-dependents	nterrogate-service	service-user-defined-control
EventLog	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac

EventLog	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
EventLog	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
EventLog	Access Allowed for Administrators	stop-service	pause-continue-service	-
EventLog	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
EventLog	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
EventLog	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
EventLog	Access Allowed for S-1-15-2-1	query-service-status	nterrogate-service	-
EventSystem	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
EventSystem	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
EventSystem	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
EventSystem	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
EventSystem	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
EventSystem	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
EventSystem	Access Allowed for Administrators	stop-service	pause-continue-service	-
EventSystem	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
EventSystem	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
EventSystem	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
EventSystem	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
fdPHost	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
fdPHost	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
fdPHost	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
fdPHost	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
fdPHost	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
fdPHost	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
fdPHost	Access Allowed for Administrators	stop-service	pause-continue-service	-
fdPHost	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
fdPHost	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
fdPHost	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
fdPHost	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FDResPub	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
FDResPub	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
FDResPub	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
FDResPub	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
FDResPub	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config

FDResPub	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
FDResPub	Access Allowed for Administrators	stop-service	pause-continue-service	-
FDResPub	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
FDResPub	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
FDResPub	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
FDResPub	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
FDResPub	Access Allowed for Network_Configuration_Operators	standard-read	query-service-config	query-service-status
FDResPub	Access Allowed for Network_Configuration_Operators	enumerate-service-dependents	start-service	stop-service
FDResPub	Access Allowed for Network_Configuration_Operators	pause-continue-service	nterrogate-service	service-user-defined-control
FontCache	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
FontCache	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
FontCache	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
FontCache	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
FontCache	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
FontCache	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
FontCache	Access Allowed for Administrators	stop-service	pause-continue-service	-
FontCache	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
FontCache	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
FontCache	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
FontCache	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
FontCache	Access Allowed for Interactive_Logon	start-service	-	-
FontCache	Access Allowed for Service_Logon	start-service	-	-
FontCache	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
FontCache	Access Allowed for S-1-15-2-1	enumerate-service-dependents	start-service	nterrogate-service
FontCache	Access Allowed for S-1-15-2-1	service-user-defined-control	-	-
gpsvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
gpsvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
gpsvc	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
gpsvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
gpsvc	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
gpsvc	Access Allowed for Administrators	enumerate-service-dependents	nterrogate-service	service-user-defined-control
gpsvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
gpsvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
gpsvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

gpsvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
IKEEXT	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
IKEEXT	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
IKEEXT	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
IKEEXT	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
IKEEXT	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
IKEEXT	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
IKEEXT	Access Allowed for Administrators	stop-service	pause-continue-service	-
IKEEXT	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
IKEEXT	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
IKEEXT	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
IKEEXT	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
InstallService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
InstallService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
InstallService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
InstallService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
InstallService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
InstallService	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
InstallService	Access Allowed for Administrators	stop-service	pause-continue-service	-
InstallService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
InstallService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
InstallService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
InstallService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
iphlpsvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
iphlpsvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
iphlpsvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
iphlpsvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
iphlpsvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
iphlpsvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
iphlpsvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
iphlpsvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
iphlpsvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
iphlpsvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
iphlpsvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

KeyIso	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
KeyIso	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
KeyIso	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
KeyIso	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
KeyIso	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
KeyIso	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
KeyIso	Access Allowed for Administrators	stop-service	pause-continue-service	-
KeyIso	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
KeyIso	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
KeyIso	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
KeyIso	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
KeyIso	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
KeyIso	Access Allowed for Service_Logon	service-user-defined-control	-	-
KeyIso	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
KeyIso	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
LanmanServer	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
LanmanServer	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
LanmanServer	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
LanmanServer	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
LanmanServer	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
LanmanServer	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
LanmanServer	Access Allowed for Administrators	stop-service	pause-continue-service	-
LanmanServer	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
LanmanServer	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
LanmanServer	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
LanmanServer	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
LanmanWorkstation	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
LanmanWorkstation	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
LanmanWorkstation	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
LanmanWorkstation	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
LanmanWorkstation	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
LanmanWorkstation	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
LanmanWorkstation	Access Allowed for Administrators	stop-service	pause-continue-service	-
LanmanWorkstation	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

LanmanWorkstation	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
LanmanWorkstation	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
LanmanWorkstation	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
lfsvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
lfsvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
lfsvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
lfsvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
lfsvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
lfsvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
lfsvc	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
lfsvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
lfsvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
lfsvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
lfsvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
lfsvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
lfsvc	Access Allowed for S-1-15-3-1024-2158456844-3754929254-744589270-3611187126-2481208986-30837703-3416168463-2437063433	query-service-status	start-service	-
lfsvc	Access Allowed for Interactive_Logon	query-service-status	start-service	-
lfsvc	Access Allowed for S-1-5-32-2158456844-3754929254-744589270-3611187126-2481208986-30837703-3416168463-2437063433	query-service-status	start-service	-
lfsvc	Access Denied for S-1-15-3-1024-3842824567-178914259-466740046-159386189-4235713590-3349026085-1947878110-3889710422	query-service-status	start-service	stop-service
lfsvc	Access Denied for Interactive_Logon	query-service-status	start-service	stop-service
lfsvc	Access Denied for S-1-5-32-3842824567-178914259-466740046-159386189-4235713590-3349026085-1947878110-3889710422	query-service-status	start-service	stop-service
LicenseManager	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
LicenseManager	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
LicenseManager	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
LicenseManager	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
LicenseManager	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
LicenseManager	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
LicenseManager	Access Allowed for Administrators	stop-service	pause-continue-service	-

LicenseManager	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
LicenseManager	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
LicenseManager	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
LicenseManager	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
lmhosts	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
lmhosts	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
lmhosts	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
lmhosts	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
lmhosts	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
lmhosts	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
lmhosts	Access Allowed for Administrators	stop-service	pause-continue-service	-
lmhosts	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
lmhosts	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
lmhosts	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
lmhosts	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
LSM	Access Allowed for Authenticated_Users	query-service-config	query-service-status	enumerate-service-de pendents
LSM	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
LSM	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
LSM	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
LSM	Access Allowed for Local_System	stop-service	pause-continue-service	-
LSM	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
LSM	Access Allowed for Administrators	enumerate-service-de pendents	nterrogate-service	-
mpssvc	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
mpssvc	Access Allowed for Authenticated_Users	nterrogate-service	-	-
mpssvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
mpssvc	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
mpssvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	nterrogate-service
mpssvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mpssvc	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
mpssvc	Access Allowed for Administrators	start-service	nterrogate-service	-
mpssvc	Access Allowed for Users	query-service-config	query-service-status	nterrogate-service
NcbService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NcbService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NcbService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control

NcbService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NcbService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NcbService	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
NcbService	Access Allowed for Administrators	stop-service	pause-continue-service	-
NcbService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NcbService	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
NcbService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NcbService	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
NcdAutoSetup	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NcdAutoSetup	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
NcdAutoSetup	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NcdAutoSetup	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NcdAutoSetup	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NcdAutoSetup	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
NcdAutoSetup	Access Allowed for Administrators	stop-service	pause-continue-service	-
NcdAutoSetup	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NcdAutoSetup	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
NcdAutoSetup	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NcdAutoSetup	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Netman	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Netman	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
Netman	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Netman	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Netman	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Netman	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
Netman	Access Allowed for Administrators	stop-service	pause-continue-service	-
Netman	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Netman	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Netman	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Netman	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
netprofm	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
netprofm	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
netprofm	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
netprofm	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac

netprofm	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
netprofm	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
netprofm	Access Allowed for Administrators	stop-service	pause-continue-service	-
netprofm	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
netprofm	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
netprofm	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
netprofm	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
NlaSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NlaSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NlaSvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
NlaSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
NlaSvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
NlaSvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
NlaSvc	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
NlaSvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
NlaSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NlaSvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
NlaSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NlaSvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
NlaSvc	Access Allowed for S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453	standard-read	query-service-config	query-service-status
NlaSvc	Access Allowed for S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453	enumerate-service-dependents	start-service	-
nsi	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
nsi	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
nsi	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
nsi	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
nsi	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
nsi	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
nsi	Access Allowed for Administrators	stop-service	pause-continue-service	-
nsi	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
nsi	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
nsi	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
nsi	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
PcaSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status

PcaSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
PcaSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
PcaSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
PcaSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
PcaSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
PcaSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
PcaSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
PcaSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
PcaSvc	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
PcaSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
PcaSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
PcaSvc	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
PlugPlay	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
PlugPlay	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
PlugPlay	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
PlugPlay	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
PlugPlay	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
PlugPlay	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
PlugPlay	Access Allowed for Administrators	stop-service	pause-continue-service	-
PlugPlay	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
PlugPlay	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
PlugPlay	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
PlugPlay	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
PolicyAgent	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
PolicyAgent	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
PolicyAgent	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
PolicyAgent	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
PolicyAgent	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
PolicyAgent	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
PolicyAgent	Access Allowed for Administrators	stop-service	pause-continue-service	-
PolicyAgent	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
PolicyAgent	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
PolicyAgent	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
PolicyAgent	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

Power	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Power	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Power	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Power	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Power	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Power	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Power	Access Allowed for Administrators	stop-service	pause-continue-service	-
Power	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Power	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Power	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Power	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ProfSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
ProfSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
ProfSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
ProfSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
ProfSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
ProfSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
ProfSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
ProfSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
ProfSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ProfSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
ProfSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
RemoteRegistry	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
RemoteRegistry	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
RemoteRegistry	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
RemoteRegistry	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
RemoteRegistry	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
RemoteRegistry	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
RemoteRegistry	Access Allowed for Administrators	stop-service	pause-continue-service	-
RemoteRegistry	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
RemoteRegistry	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
RemoteRegistry	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
RemoteRegistry	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
RmSvc	Access Allowed for Local_Service	standard-read	query-service-config	query-service-status

RmSvc	Access Allowed for Local_Service	enumerate-service-de pendents	start-service	stop-service
RmSvc	Access Allowed for Local_Service	pause-continue-service	nterrogate-service	service-user-defined-control
RmSvc	Access Allowed for Local_System	standard-read	query-service-config	change-service-config
RmSvc	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
RmSvc	Access Allowed for Local_System	stop-service	pause-continue-service	nterrogate-service
RmSvc	Access Allowed for Local_System	service-user-defined-control	-	-
RmSvc	Access Allowed for Administrators	standard-read	query-service-config	change-service-config
RmSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
RmSvc	Access Allowed for Administrators	stop-service	pause-continue-service	nterrogate-service
RmSvc	Access Allowed for Administrators	service-user-defined-control	-	-
RmSvc	Access Allowed for Users	standard-read	query-service-config	query-service-status
RmSvc	Access Allowed for Users	enumerate-service-de pendents	start-service	stop-service
RmSvc	Access Allowed for Users	pause-continue-service	nterrogate-service	service-user-defined-control
RpcEptMapper	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
RpcEptMapper	Access Allowed for Authenticated_Users	nterrogate-service	-	-
RpcEptMapper	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
RpcEptMapper	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
RpcEptMapper	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
RpcEptMapper	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
RpcEptMapper	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
RpcEptMapper	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
RpcEptMapper	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
RpcEptMapper	Access Allowed for Administrators	nterrogate-service	-	-
RpcEptMapper	Access Allowed for Users	query-service-config	query-service-status	start-service
RpcEptMapper	Access Allowed for Users	nterrogate-service	-	-
RpcSs	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
RpcSs	Access Allowed for Authenticated_Users	nterrogate-service	-	-
RpcSs	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
RpcSs	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
RpcSs	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
RpcSs	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
RpcSs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
RpcSs	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
RpcSs	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
RpcSs	Access Allowed for Administrators	nterrogate-service	-	-
RpcSs	Access Allowed for Users	query-service-config	query-service-status	nterrogate-service

SamSs	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
SamSs	Access Allowed for Authenticated_Users	enumerate-service-dependents	nterrogate-service	-
SamSs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SamSs	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
SamSs	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
SamSs	Access Allowed for Administrators	stop-service	pause-continue-service	-
SamSs	Access Allowed for Interactive_Logon	query-service-config	query-service-status	enumerate-service-dependents
SamSs	Access Allowed for Interactive_Logon	nterrogate-service	-	-
SamSs	Access Allowed for Users	query-service-config	query-service-status	enumerate-service-dependents
SamSs	Access Allowed for Users	nterrogate-service	-	-
Schedule	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
Schedule	Access Allowed for Authenticated_Users	enumerate-service-dependents	nterrogate-service	-
Schedule	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Schedule	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-dependents
Schedule	Access Allowed for Administrators	start-service	pause-continue-service	nterrogate-service
Schedule	Access Allowed for Administrators	service-user-defined-control	-	-
Schedule	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
Schedule	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
Schedule	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
Schedule	Access Allowed for Local_System	stop-service	pause-continue-service	-
Schedule	Access Allowed for Users	standard-read	query-service-config	query-service-status
Schedule	Access Allowed for Users	enumerate-service-dependents	nterrogate-service	-
SecurityHealthService	Access Allowed for Users	standard-read	query-service-config	query-service-status
SecurityHealthService	Access Allowed for Users	enumerate-service-dependents	start-service	nterrogate-service
SecurityHealthService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
SecurityHealthService	Access Allowed for Local_System	enumerate-service-dependents	start-service	nterrogate-service
SecurityHealthService	Access Allowed for Local_System	service-user-defined-control	-	-
SecurityHealthService	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
SecurityHealthService	Access Allowed for Administrators	enumerate-service-dependents	start-service	nterrogate-service
SecurityHealthService	Access Allowed for Administrators	service-user-defined-control	-	-
SecurityHealthService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SecurityHealthService	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
SecurityHealthService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
SecurityHealthService	Access Allowed for Service_Logon	enumerate-service-dependents	start-service	nterrogate-service
SecurityHealthService	Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977	standard-read	query-service-config	query-service-status

	361409-3075122917			
SecurityHealthService	Access Allowed for S-1-5-80-1601830629-99 0752416-3372939810-977 361409-3075122917	enumerate-service-de pendents	start-service	stop-service
SecurityHealthService	Access Allowed for S-1-5-80-1601830629-99 0752416-3372939810-977 361409-3075122917	pause-continue-service	nterrogate-service	service-user-defined-control
SecurityHealthService	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-read	standard-write-owner	standard-write-dac
SecurityHealthService	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-delete	query-service-config	change-service-config
SecurityHealthService	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	query-service-status	enumerate-service-de pendents	start-service
SecurityHealthService	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	stop-service	pause-continue-service	-
SecurityHealthService	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	standard-read	standard-write-owner	standard-write-dac
SecurityHealthService	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	standard-delete	query-service-config	change-service-config
SecurityHealthService	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	query-service-status	enumerate-service-de pendents	start-service
SecurityHealthService	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	stop-service	pause-continue-service	-
SEMgrSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SEMgrSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
SEMgrSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
SEMgrSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
SEMgrSvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
SEMgrSvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
SEMgrSvc	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
SEMgrSvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
SEMgrSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SEMgrSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
SEMgrSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
SEMgrSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
SEMgrSvc	Access Allowed for S-1-15-2-1	query-service-status	-	-
SEMgrSvc	Access Allowed for Interactive_Logon	query-service-status	-	-
SEMgrSvc	Access Allowed for Authenticated_Users	query-service-status	-	-
SEMgrSvc	Access Denied for S-1-15-3-1024-21692379 47-275284851-387635746	start-service	stop-service	-

	0-1273727642-1157490466-1177376558-883687086-945396102			
SEMgrSvc	Access Denied for Interactive_Logon	start-service	stop-service	-
SEMgrSvc	Access Denied for S-1-5-32-2169237947-275284851-3876357460-1273727642-1157490466-1177376558-883687086-945396102	start-service	stop-service	-
SENS	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
SENS	Access Allowed for Authenticated_Users	enumerate-service-dependents	nterrogate-service	service-user-defined-control
SENS	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SENS	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
SENS	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
SENS	Access Allowed for Administrators	stop-service	pause-continue-service	-
SENS	Access Allowed for System_Operators	query-service-config	query-service-status	enumerate-service-dependents
SENS	Access Allowed for System_Operators	start-service	stop-service	pause-continue-service
SENS	Access Allowed for System_Operators	nterrogate-service	service-user-defined-control	-
SENS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
SENS	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
SENS	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
SENS	Access Allowed for S-1-15-2-1	standard-read	query-service-status	nterrogate-service
SgrmBroker	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
SgrmBroker	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
SgrmBroker	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
SgrmBroker	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SgrmBroker	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
SgrmBroker	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
SgrmBroker	Access Allowed for Administrators	stop-service	pause-continue-service	-
SgrmBroker	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SgrmBroker	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
SgrmBroker	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
SgrmBroker	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
ShellHWDetection	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
ShellHWDetection	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
ShellHWDetection	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
ShellHWDetection	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
ShellHWDetection	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
ShellHWDetection	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service

ShellHWDetection	Access Allowed for Administrators	stop-service	pause-continue-service	-
ShellHWDetection	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
ShellHWDetection	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
ShellHWDetection	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
ShellHWDetection	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Spooler	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
Spooler	Access Allowed for Authenticated_Users	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Spooler	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Spooler	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Spooler	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
Spooler	Access Allowed for Administrators	stop-service	pause-continue-service	-
Spooler	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Spooler	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
Spooler	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
SSDPSRV	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
SSDPSRV	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
SSDPSRV	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
SSDPSRV	Access Allowed for Local_System	stop-service	pause-continue-service	-
SSDPSRV	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SSDPSRV	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
SSDPSRV	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
SSDPSRV	Access Allowed for Administrators	stop-service	pause-continue-service	-
SSDPSRV	Access Allowed for System_Operators	standard-read	query-service-config	query-service-status
SSDPSRV	Access Allowed for System_Operators	enumerate-service-dependents	start-service	stop-service
SSDPSRV	Access Allowed for System_Operators	nterrogate-service	-	-
SSDPSRV	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SSDPSRV	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
SSDPSRV	Access Allowed for Local_Service	standard-read	query-service-config	query-service-status
SSDPSRV	Access Allowed for Local_Service	enumerate-service-dependents	start-service	stop-service
SSDPSRV	Access Allowed for Local_Service	pause-continue-service	nterrogate-service	service-user-defined-control
SSDPSRV	Access Allowed for Network_Service	standard-read	query-service-config	query-service-status
SSDPSRV	Access Allowed for Network_Service	enumerate-service-dependents	start-service	stop-service
SSDPSRV	Access Allowed for Network_Service	pause-continue-service	nterrogate-service	service-user-defined-control
StateRepository	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-185	standard-read	standard-write-owner	standard-write-dac

	3292631-2271478464			
StateRepository	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	standard-delete	query-service-config	change-service-config
StateRepository	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	query-service-status	enumerate-service-dependents	start-service
StateRepository	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	stop-service	pause-continue-service	-
StateRepository	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
StateRepository	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
StateRepository	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
StateRepository	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
StateRepository	Access Allowed for Administrators	enumerate-service-dependents	start-service	stop-service
StateRepository	Access Allowed for Administrators	pause-continue-service	nterrogate-service	service-user-defined-control
StateRepository	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
StateRepository	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
StateRepository	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
StateRepository	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
StateRepository	Access Allowed for Service_Logon	enumerate-service-dependents	start-service	nterrogate-service
StateRepository	Access Allowed for Service_Logon	service-user-defined-control	-	-
StateRepository	Access Allowed for S-1-15-2-1	query-service-status	start-service	-
StorSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
StorSvc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
StorSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
StorSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
StorSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
StorSvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
StorSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
StorSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
StorSvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
StorSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
StorSvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
SysMain	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
SysMain	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
SysMain	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
SysMain	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SysMain	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config

SysMain	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
SysMain	Access Allowed for Administrators	stop-service	pause-continue-service	-
SysMain	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SysMain	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
SysMain	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
SysMain	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
SystemEventsBroker	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
SystemEventsBroker	Access Allowed for Authenticated_Users	nterrogate-service	-	-
SystemEventsBroker	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
SystemEventsBroker	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
SystemEventsBroker	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
SystemEventsBroker	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
SystemEventsBroker	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SystemEventsBroker	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
SystemEventsBroker	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
SystemEventsBroker	Access Allowed for Administrators	nterrogate-service	-	-
SystemEventsBroker	Access Allowed for Users	query-service-config	query-service-status	start-service
SystemEventsBroker	Access Allowed for Users	nterrogate-service	-	-
TabletInputService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
TabletInputService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
TabletInputService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
TabletInputService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
TabletInputService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
TabletInputService	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
TabletInputService	Access Allowed for Administrators	stop-service	pause-continue-service	-
TabletInputService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
TabletInputService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TabletInputService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
TabletInputService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TabletInputService	Access Allowed for All	start-service	-	-
Themes	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Themes	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Themes	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Themes	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Themes	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config

Themes	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Themes	Access Allowed for Administrators	stop-service	pause-continue-service	-
Themes	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Themes	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Themes	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Themes	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TimeBrokerSvc	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
TimeBrokerSvc	Access Allowed for Authenticated_Users	nterrogate-service	-	-
TimeBrokerSvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
TimeBrokerSvc	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
TimeBrokerSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
TimeBrokerSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	-
TimeBrokerSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
TimeBrokerSvc	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
TimeBrokerSvc	Access Allowed for Administrators	start-service	stop-service	pause-continue-service
TimeBrokerSvc	Access Allowed for Administrators	nterrogate-service	-	-
TimeBrokerSvc	Access Allowed for Users	query-service-config	query-service-status	start-service
TimeBrokerSvc	Access Allowed for Users	nterrogate-service	-	-
TokenBroker	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
TokenBroker	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
TokenBroker	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
TokenBroker	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
TokenBroker	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
TokenBroker	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
TokenBroker	Access Allowed for Administrators	stop-service	pause-continue-service	-
TokenBroker	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
TokenBroker	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TokenBroker	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
TokenBroker	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TrkWks	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
TrkWks	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
TrkWks	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
TrkWks	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
TrkWks	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
TrkWks	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service

TrkWks	Access Allowed for Administrators	stop-service	pause-continue-service	-
TrkWks	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
TrkWks	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
TrkWks	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
TrkWks	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
UserManager	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
UserManager	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
UserManager	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
UserManager	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
UserManager	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
UserManager	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
UserManager	Access Allowed for Administrators	stop-service	pause-continue-service	-
UserManager	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
UserManager	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
UserManager	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
UserManager	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
UsoSvc	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
UsoSvc	Access Allowed for Authenticated_Users	enumerate-service-de pendents	start-service	nterrogate-service
UsoSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
UsoSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
UsoSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
UsoSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
UsoSvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
UsoSvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
UsoSvc	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
UsoSvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
VaultSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
VaultSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
VaultSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
VaultSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
VaultSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
VaultSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
VaultSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
VaultSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

VaultSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
VaultSvc	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
VaultSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
VaultSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
VaultSvc	Access Allowed for Service_Logon	service-user-defined-control	-	-
VaultSvc	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
VaultSvc	Access Allowed for Network_Service	query-service-status	start-service	-
VaultSvc	Access Allowed for Local_Service	query-service-status	start-service	-
VaultSvc	Access Allowed for S-1-15-2-1	query-service-status	start-service	-
VBoxService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
VBoxService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
VBoxService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
VBoxService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
VBoxService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
VBoxService	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
VBoxService	Access Allowed for Administrators	stop-service	pause-continue-service	-
VBoxService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
VBoxService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
VBoxService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
VBoxService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
WaaSMedicSvc	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
WaaSMedicSvc	Access Allowed for Authenticated_Users	enumerate-service-de pendents	start-service	nterrogate-service
WaaSMedicSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
WaaSMedicSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
WaaSMedicSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
WaaSMedicSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
WaaSMedicSvc	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
WaaSMedicSvc	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
WaaSMedicSvc	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
WaaSMedicSvc	Access Allowed for Local_System	stop-service	pause-continue-service	-
WbioSrvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
WbioSrvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
WbioSrvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
WbioSrvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac

WbioSrvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
WbioSrvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
WbioSrvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
WbioSrvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WbioSrvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
WbioSrvc	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
WbioSrvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
WbioSrvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
WbioSrvc	Access Allowed for Authenticated_Users	service-user-defined-control	-	-
WbioSrvc	Access Allowed for S-1-15-2-1	query-service-config	query-service-status	start-service
Wcmsvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Wcmsvc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
Wcmsvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Wcmsvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Wcmsvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Wcmsvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
Wcmsvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
Wcmsvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Wcmsvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Wcmsvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Wcmsvc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
WdiServiceHost	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
WdiServiceHost	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
WdiServiceHost	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
WdiServiceHost	Access Allowed for Local_System	stop-service	pause-continue-service	-
WdiServiceHost	Access Allowed for Administrators	standard-read	query-service-config	change-service-config
WdiServiceHost	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	stop-service
WdiServiceHost	Access Allowed for Administrators	pause-continue-service	nterrogate-service	service-user-defined-control
WdiServiceHost	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WdiServiceHost	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
WdiServiceHost	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
WdiServiceHost	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
WdiServiceHost	Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-1451644582	standard-read	query-service-config	query-service-status
WdiServiceHost	Access Allowed for S-1-5-80-2970612574-78	enumerate-service-dependents	start-service	stop-service

	537857-698502321-55867 4196-1451644582			
WdiServiceHost	Access Allowed for S-1-5-80-2970612574-78 537857-698502321-55867 4196-1451644582	pause-continue-service	nterrogate-service	service-user-defined-control
WdNisSvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
WdNisSvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
WdNisSvc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
WdNisSvc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
WdNisSvc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
WdNisSvc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
WdNisSvc	Access Allowed for Administrators	stop-service	pause-continue-service	-
WdNisSvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WdNisSvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
WdNisSvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
WdNisSvc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
WinDefend	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-read	standard-write-owner	standard-write-dac
WinDefend	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-delete	query-service-config	change-service-config
WinDefend	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	query-service-status	enumerate-service-de pendents	start-service
WinDefend	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	stop-service	pause-continue-service	-
WinDefend	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	generic-all	-	-
WinDefend	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
WinDefend	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
WinDefend	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
WinDefend	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
WinDefend	Access Allowed for Administrators	query-service-config	change-service-config	query-service-status
WinDefend	Access Allowed for Administrators	enumerate-service-de pendents	start-service	stop-service
WinDefend	Access Allowed for Administrators	pause-continue-service	nterrogate-service	-
WinDefend	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WinDefend	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
WinDefend	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
WinDefend	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

WinDefend	Access Allowed for Service_Logon	enumerate-service-dependents	start-service	nterrogate-service
WinDefend	Access Allowed for Service_Logon	service-user-defined-control	-	-
WinHttpAutoProxySvc	Access Allowed for Local_System	standard-read	standard-delete	query-service-config
WinHttpAutoProxySvc	Access Allowed for Local_System	query-service-status	enumerate-service-dependents	start-service
WinHttpAutoProxySvc	Access Allowed for Local_System	nterrogate-service	-	-
WinHttpAutoProxySvc	Access Allowed for Administrators	standard-read	standard-delete	query-service-config
WinHttpAutoProxySvc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
WinHttpAutoProxySvc	Access Allowed for Administrators	nterrogate-service	-	-
WinHttpAutoProxySvc	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
WinHttpAutoProxySvc	Access Allowed for Authenticated_Users	enumerate-service-dependents	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WinHttpAutoProxySvc	Access Allowed for Interactive_Logon	enumerate-service-dependents	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
WinHttpAutoProxySvc	Access Allowed for Service_Logon	enumerate-service-dependents	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for S-1-15-2-1	query-service-status	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for S-1-15-3-1	query-service-status	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for S-1-15-3-2	query-service-status	start-service	nterrogate-service
WinHttpAutoProxySvc	Access Allowed for S-1-15-3-3	query-service-status	start-service	nterrogate-service
Winmgmt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Winmgmt	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
Winmgmt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Winmgmt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Winmgmt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Winmgmt	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
Winmgmt	Access Allowed for Administrators	stop-service	pause-continue-service	-
Winmgmt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Winmgmt	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Winmgmt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Winmgmt	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
WpnService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
WpnService	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
WpnService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
WpnService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
WpnService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
WpnService	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
WpnService	Access Allowed for Administrators	stop-service	pause-continue-service	-

WpnService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
WpnService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
WpnService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
WpnService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
wscsvc	Access Allowed for Users	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for Users	enumerate-service-de pendents	start-service	nterrogate-service
wscsvc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	nterrogate-service
wscsvc	Access Allowed for Local_System	service-user-defined-control	-	-
wscsvc	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for Administrators	enumerate-service-de pendents	start-service	nterrogate-service
wscsvc	Access Allowed for Administrators	service-user-defined-control	-	-
wscsvc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
wscsvc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
wscsvc	Access Allowed for S-1-5-80-1601830629-99 0752416-3372939810-977 361409-3075122917	standard-read	query-service-config	query-service-status
wscsvc	Access Allowed for S-1-5-80-1601830629-99 0752416-3372939810-977 361409-3075122917	enumerate-service-de pendents	start-service	stop-service
wscsvc	Access Allowed for S-1-5-80-1601830629-99 0752416-3372939810-977 361409-3075122917	pause-continue-service	nterrogate-service	service-user-defined-control
wscsvc	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-read	standard-write-owner	standard-write-dac
wscsvc	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	standard-delete	query-service-config	change-service-config
wscsvc	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	query-service-status	enumerate-service-de pendents	start-service
wscsvc	Access Allowed for S-1-5-80-956008885-341 8522649-1831038044-185 3292631-2271478464	stop-service	pause-continue-service	-
wscsvc	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	standard-read	standard-write-owner	standard-write-dac
wscsvc	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	standard-delete	query-service-config	change-service-config
wscsvc	Access Allowed for S-1-5-80-259296475-408 4429506-1152984619-387 39575-565535606	query-service-status	enumerate-service-de pendents	start-service
wscsvc	Access Allowed for S-1-5-80-259296475-408	stop-service	pause-continue-service	-

	4429506-1152984619-387 39575-565535606			
WSearch	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
WSearch	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
WSearch	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
WSearch	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
WSearch	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Results were truncated.				

2 Microsoft Windows Driver Security Analysis

QID:	105184
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This test enumerates the security permissions for driver objects on the target Windows system.

IMPACT:

Improper driver object security can let an unauthorized user control critical operating system components.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Access	ACL1	ACL2	ACL3
ACPI	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
ACPI	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
ACPI	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
ACPI	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
ACPI	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
ACPI	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
ACPI	Access Allowed for Administrators	stop-service	pause-continue-service	-

ACPI	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
ACPI	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ACPI	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
ACPI	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
acpiex	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
acpiex	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
acpiex	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
acpiex	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
acpiex	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
acpiex	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
acpiex	Access Allowed for Administrators	stop-service	pause-continue-service	-
acpiex	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
acpiex	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
acpiex	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
acpiex	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
AFD	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
AFD	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
AFD	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
AFD	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
AFD	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
AFD	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
AFD	Access Allowed for Administrators	stop-service	pause-continue-service	-
AFD	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
AFD	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
AFD	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
AFD	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
afunix	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
afunix	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
afunix	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
afunix	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
afunix	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
afunix	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
afunix	Access Allowed for Administrators	stop-service	pause-continue-service	-
afunix	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

afunix	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
afunix	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
afunix	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ahcache	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
ahcache	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
ahcache	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
ahcache	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
ahcache	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
ahcache	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
ahcache	Access Allowed for Administrators	stop-service	pause-continue-service	-
ahcache	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
ahcache	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ahcache	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
ahcache	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bam	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
bam	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
bam	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
bam	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
bam	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
bam	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
bam	Access Allowed for Administrators	stop-service	pause-continue-service	-
bam	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
bam	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bam	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
bam	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
BasicDisplay	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
BasicDisplay	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
BasicDisplay	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
BasicDisplay	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
BasicDisplay	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
BasicDisplay	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
BasicDisplay	Access Allowed for Administrators	stop-service	pause-continue-service	-
BasicDisplay	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
BasicDisplay	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

BasicDisplay	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
BasicDisplay	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
BasicRender	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
BasicRender	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
BasicRender	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
BasicRender	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
BasicRender	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
BasicRender	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
BasicRender	Access Allowed for Administrators	stop-service	pause-continue-service	-
BasicRender	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
BasicRender	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
BasicRender	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
BasicRender	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Beep	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Beep	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Beep	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Beep	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Beep	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Beep	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Beep	Access Allowed for Administrators	stop-service	pause-continue-service	-
Beep	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Beep	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Beep	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Beep	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bindflt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
bindflt	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
bindflt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
bindflt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
bindflt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
bindflt	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
bindflt	Access Allowed for Administrators	stop-service	pause-continue-service	-
bindflt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
bindflt	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bindflt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

bindflt	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bowser	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
bowser	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
bowser	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
bowser	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
bowser	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
bowser	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
bowser	Access Allowed for Administrators	stop-service	pause-continue-service	-
bowser	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
bowser	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
bowser	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
bowser	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CAD	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CAD	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CAD	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CAD	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CAD	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CAD	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CAD	Access Allowed for Administrators	stop-service	pause-continue-service	-
CAD	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CAD	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CAD	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CAD	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
cdfs	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
cdfs	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
cdfs	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
cdfs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
cdfs	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
cdfs	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
cdfs	Access Allowed for Administrators	stop-service	pause-continue-service	-
cdfs	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
cdfs	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
cdfs	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
cdfs	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

cdrom	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
cdrom	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
cdrom	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
cdrom	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
cdrom	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
cdrom	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
cdrom	Access Allowed for Administrators	stop-service	pause-continue-service	-
cdrom	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
cdrom	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
cdrom	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
cdrom	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CimFS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CimFS	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CimFS	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CimFS	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CimFS	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CimFS	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CimFS	Access Allowed for Administrators	stop-service	pause-continue-service	-
CimFS	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CimFS	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CimFS	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CimFS	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CldFlt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CldFlt	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CldFlt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CldFlt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CldFlt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CldFlt	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CldFlt	Access Allowed for Administrators	stop-service	pause-continue-service	-
CldFlt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CldFlt	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CldFlt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CldFlt	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CLFS	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532	standard-read	standard-write-owner	standard-write-dac

	92631-2271478464			
CLFS	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	standard-delete	query-service-config	change-service-config
CLFS	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	query-service-status	enumerate-service-dependents	start-service
CLFS	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	stop-service	pause-continue-service	-
CLFS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CLFS	Access Allowed for Local_System	enumerate-service-dependents	nterrogate-service	-
CLFS	Access Allowed for Administrators	standard-read	query-service-config	query-service-status
CLFS	Access Allowed for Administrators	enumerate-service-dependents	nterrogate-service	-
CLFS	Access Allowed for Users	standard-read	query-service-config	query-service-status
CLFS	Access Allowed for Users	enumerate-service-dependents	nterrogate-service	-
CLFS	Access Allowed for S-1-15-2-1	standard-read	query-service-config	query-service-status
CLFS	Access Allowed for S-1-15-2-1	enumerate-service-dependents	nterrogate-service	-
CLFS	Access Allowed for S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	standard-read	query-service-config	query-service-status
CLFS	Access Allowed for S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681	enumerate-service-dependents	nterrogate-service	-
CmBatt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CmBatt	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
CmBatt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CmBatt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CmBatt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CmBatt	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
CmBatt	Access Allowed for Administrators	stop-service	pause-continue-service	-
CmBatt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CmBatt	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
CmBatt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CmBatt	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
CNG	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CNG	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
CNG	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CNG	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CNG	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config

CNG	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CNG	Access Allowed for Administrators	stop-service	pause-continue-service	-
CNG	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CNG	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CNG	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CNG	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CompositeBus	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CompositeBus	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CompositeBus	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CompositeBus	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CompositeBus	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CompositeBus	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
CompositeBus	Access Allowed for Administrators	stop-service	pause-continue-service	-
CompositeBus	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CompositeBus	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CompositeBus	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CompositeBus	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
condrv	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
condrv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
condrv	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
condrv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
condrv	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
condrv	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
condrv	Access Allowed for Administrators	stop-service	pause-continue-service	-
condrv	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
condrv	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
condrv	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
condrv	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CSC	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
CSC	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
CSC	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
CSC	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
CSC	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
CSC	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service

CSC	Access Allowed for Administrators	stop-service	pause-continue-service	-
CSC	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
CSC	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
CSC	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
CSC	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Dfsc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Dfsc	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Dfsc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Dfsc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Dfsc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Dfsc	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Dfsc	Access Allowed for Administrators	stop-service	pause-continue-service	-
Dfsc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Dfsc	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Dfsc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Dfsc	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
disk	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
disk	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
disk	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
disk	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
disk	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
disk	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
disk	Access Allowed for Administrators	stop-service	pause-continue-service	-
disk	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
disk	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
disk	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
disk	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
DXGKrnl	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
DXGKrnl	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
DXGKrnl	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
DXGKrnl	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
DXGKrnl	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
DXGKrnl	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
DXGKrnl	Access Allowed for Administrators	stop-service	pause-continue-service	-

DXGKrnl	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
DXGKrnl	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
DXGKrnl	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
DXGKrnl	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
E1G60	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
E1G60	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
E1G60	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
E1G60	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
E1G60	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
E1G60	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
E1G60	Access Allowed for Administrators	stop-service	pause-continue-service	-
E1G60	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
E1G60	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
E1G60	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
E1G60	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
EhStorClass	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
EhStorClass	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
EhStorClass	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
EhStorClass	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
EhStorClass	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
EhStorClass	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
EhStorClass	Access Allowed for Administrators	stop-service	pause-continue-service	-
EhStorClass	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
EhStorClass	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
EhStorClass	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
EhStorClass	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FileCrypt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
FileCrypt	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
FileCrypt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
FileCrypt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
FileCrypt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
FileCrypt	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
FileCrypt	Access Allowed for Administrators	stop-service	pause-continue-service	-
FileCrypt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

FileCrypt	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FileCrypt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
FileCrypt	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FileInfo	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
FileInfo	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
FileInfo	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
FileInfo	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
FileInfo	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
FileInfo	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
FileInfo	Access Allowed for Administrators	stop-service	pause-continue-service	-
FileInfo	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
FileInfo	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FileInfo	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
FileInfo	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FltMgr	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
FltMgr	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
FltMgr	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
FltMgr	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
FltMgr	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
FltMgr	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
FltMgr	Access Allowed for Administrators	stop-service	pause-continue-service	-
FltMgr	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
FltMgr	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
FltMgr	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
FltMgr	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
fvevol	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
fvevol	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
fvevol	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
fvevol	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
fvevol	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
fvevol	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
fvevol	Access Allowed for Administrators	stop-service	pause-continue-service	-
fvevol	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
fvevol	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

fvevol	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
fvevol	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
GpuEnergyDrv	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
GpuEnergyDrv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
GpuEnergyDrv	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
GpuEnergyDrv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
GpuEnergyDrv	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
GpuEnergyDrv	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
GpuEnergyDrv	Access Allowed for Administrators	stop-service	pause-continue-service	-
GpuEnergyDrv	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
GpuEnergyDrv	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
GpuEnergyDrv	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
GpuEnergyDrv	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HdAudAddService	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
HdAudAddService	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
HdAudAddService	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
HdAudAddService	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
HdAudAddService	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
HdAudAddService	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
HdAudAddService	Access Allowed for Administrators	stop-service	pause-continue-service	-
HdAudAddService	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
HdAudAddService	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HdAudAddService	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
HdAudAddService	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HDAudBus	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
HDAudBus	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
HDAudBus	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
HDAudBus	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
HDAudBus	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
HDAudBus	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
HDAudBus	Access Allowed for Administrators	stop-service	pause-continue-service	-
HDAudBus	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
HDAudBus	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HDAudBus	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

HDAudBus	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HidUsb	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
HidUsb	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
HidUsb	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
HidUsb	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
HidUsb	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
HidUsb	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
HidUsb	Access Allowed for Administrators	stop-service	pause-continue-service	-
HidUsb	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
HidUsb	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HidUsb	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
HidUsb	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
HTTP	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
HTTP	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
HTTP	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
HTTP	Access Allowed for Local_System	stop-service	pause-continue-service	-
HTTP	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
HTTP	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
HTTP	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
HTTP	Access Allowed for Administrators	stop-service	pause-continue-service	-
HTTP	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
HTTP	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
HTTP	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
HTTP	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
HTTP	Access Allowed for Batch_Logon	standard-read	query-service-config	query-service-status
HTTP	Access Allowed for Batch_Logon	enumerate-service-de pendents	start-service	nterrogate-service
i8042prt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
i8042prt	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
i8042prt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
i8042prt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
i8042prt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
i8042prt	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
i8042prt	Access Allowed for Administrators	stop-service	pause-continue-service	-
i8042prt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

i8042prt	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
i8042prt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
i8042prt	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
intelpep	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
intelpep	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
intelpep	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
intelpep	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
intelpep	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
intelpep	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
intelpep	Access Allowed for Administrators	stop-service	pause-continue-service	-
intelpep	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
intelpep	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
intelpep	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
intelpep	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
intelppm	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
intelppm	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
intelppm	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
intelppm	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
intelppm	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
intelppm	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
intelppm	Access Allowed for Administrators	stop-service	pause-continue-service	-
intelppm	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
intelppm	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
intelppm	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
intelppm	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
iorate	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
iorate	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
iorate	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
iorate	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
iorate	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
iorate	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
iorate	Access Allowed for Administrators	stop-service	pause-continue-service	-
iorate	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
iorate	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

iorate	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
iorate	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
kbdclass	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
kbdclass	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
kbdclass	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
kbdclass	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
kbdclass	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
kbdclass	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
kbdclass	Access Allowed for Administrators	stop-service	pause-continue-service	-
kbdclass	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
kbdclass	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
kbdclass	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
kbdclass	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
kdnic	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
kdnic	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
kdnic	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
kdnic	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
kdnic	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
kdnic	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
kdnic	Access Allowed for Administrators	stop-service	pause-continue-service	-
kdnic	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
kdnic	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
kdnic	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
kdnic	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
KSecDD	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
KSecDD	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
KSecDD	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
KSecDD	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
KSecDD	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
KSecDD	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
KSecDD	Access Allowed for Administrators	stop-service	pause-continue-service	-
KSecDD	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
KSecDD	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
KSecDD	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

KSecDD	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
KSecPkg	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
KSecPkg	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
KSecPkg	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
KSecPkg	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
KSecPkg	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
KSecPkg	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
KSecPkg	Access Allowed for Administrators	stop-service	pause-continue-service	-
KSecPkg	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
KSecPkg	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
KSecPkg	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
KSecPkg	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ksthunk	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
ksthunk	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
ksthunk	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
ksthunk	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
ksthunk	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
ksthunk	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
ksthunk	Access Allowed for Administrators	stop-service	pause-continue-service	-
ksthunk	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
ksthunk	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
ksthunk	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
ksthunk	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
lltdio	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
lltdio	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
lltdio	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
lltdio	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
lltdio	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
lltdio	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
lltdio	Access Allowed for Administrators	stop-service	pause-continue-service	-
lltdio	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
lltdio	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
lltdio	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
lltdio	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

luafv	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
luafv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
luafv	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
luafv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
luafv	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
luafv	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
luafv	Access Allowed for Administrators	stop-service	pause-continue-service	-
luafv	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
luafv	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
luafv	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
luafv	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
MMCSS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
MMCSS	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
MMCSS	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
MMCSS	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
MMCSS	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
MMCSS	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
MMCSS	Access Allowed for Administrators	stop-service	pause-continue-service	-
MMCSS	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
MMCSS	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
MMCSS	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
MMCSS	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
MMCSS	Access Allowed for Users	start-service	-	-
MMCSS	Access Allowed for S-1-15-2-1	query-service-status	start-service	-
monitor	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
monitor	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
monitor	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
monitor	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
monitor	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
monitor	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
monitor	Access Allowed for Administrators	stop-service	pause-continue-service	-
monitor	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
monitor	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
monitor	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
monitor	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

mouclass	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mouclass	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mouclass	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mouclass	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mouclass	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mouclass	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mouclass	Access Allowed for Administrators	stop-service	pause-continue-service	-
mouclass	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mouclass	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mouclass	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mouclass	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mouhid	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mouhid	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mouhid	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mouhid	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mouhid	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mouhid	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mouhid	Access Allowed for Administrators	stop-service	pause-continue-service	-
mouhid	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mouhid	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mouhid	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mouhid	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mountmgr	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mountmgr	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mountmgr	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mountmgr	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mountmgr	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mountmgr	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mountmgr	Access Allowed for Administrators	stop-service	pause-continue-service	-
mountmgr	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mountmgr	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mountmgr	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mountmgr	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mpsdrv	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status

mpsdrv	Access Allowed for Authenticated_Users	nterrogate-service	-	-
mpsdrv	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
mpsdrv	Access Allowed for Local_System	query-service-config	change-service-config	query-service-status
mpsdrv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	nterrogate-service
mpsdrv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mpsdrv	Access Allowed for Administrators	query-service-config	query-service-status	enumerate-service-de pendents
mpsdrv	Access Allowed for Administrators	start-service	nterrogate-service	-
mpsdrv	Access Allowed for Users	query-service-config	query-service-status	nterrogate-service
mrxsmb	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mrxsmb	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mrxsmb	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mrxsmb	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mrxsmb	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mrxsmb	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mrxsmb	Access Allowed for Administrators	stop-service	pause-continue-service	-
mrxsmb	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mrxsmb	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mrxsmb	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mrxsmb	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mrxsmb20	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mrxsmb20	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mrxsmb20	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mrxsmb20	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mrxsmb20	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mrxsmb20	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mrxsmb20	Access Allowed for Administrators	stop-service	pause-continue-service	-
mrxsmb20	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mrxsmb20	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mrxsmb20	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mrxsmb20	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Msfs	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Msfs	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Msfs	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Msfs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac

Msfs	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Msfs	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Msfs	Access Allowed for Administrators	stop-service	pause-continue-service	-
Msfs	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Msfs	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Msfs	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Msfs	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
msisadrv	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
msisadrv	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
msisadrv	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
msisadrv	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
msisadrv	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
msisadrv	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
msisadrv	Access Allowed for Administrators	stop-service	pause-continue-service	-
msisadrv	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
msisadrv	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
msisadrv	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
msisadrv	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
MsLldp	Access Denied for Guests	standard-read	standard-write-owner	standard-write-dac
MsLldp	Access Denied for Guests	standard-delete	query-service-config	change-service-config
MsLldp	Access Denied for Guests	query-service-status	enumerate-service-de pendents	start-service
MsLldp	Access Denied for Guests	stop-service	pause-continue-service	-
MsLldp	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
MsLldp	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
MsLldp	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
MsLldp	Access Allowed for Local_System	stop-service	pause-continue-service	-
MsLldp	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
MsLldp	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
MsLldp	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
MsLldp	Access Allowed for Administrators	pause-continue-service	nterrogate-service	-
MsLldp	Access Allowed for System_Operators	standard-read	query-service-config	query-service-status
MsLldp	Access Allowed for System_Operators	enumerate-service-de pendents	start-service	stop-service
MsLldp	Access Allowed for System_Operators	pause-continue-service	nterrogate-service	service-user-defined-control
MsLldp	Access Allowed for S-1-5-80-3141615172-205 7878085-1754447212-2405 740020-3916490453	query-service-status	start-service	stop-service

MsQuic	Access Allowed for Local_System	standard-read	standard-write-owner	standard-write-dac
MsQuic	Access Allowed for Local_System	standard-delete	query-service-config	change-service-config
MsQuic	Access Allowed for Local_System	query-service-status	enumerate-service-de pendents	start-service
MsQuic	Access Allowed for Local_System	stop-service	pause-continue-service	-
MsQuic	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
MsQuic	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
MsQuic	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
MsQuic	Access Allowed for Administrators	stop-service	pause-continue-service	-
MsQuic	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
MsQuic	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
MsQuic	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
MsQuic	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
MsQuic	Access Allowed for Batch_Logon	standard-read	query-service-config	query-service-status
MsQuic	Access Allowed for Batch_Logon	enumerate-service-de pendents	start-service	nterrogate-service
MsSecCore	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532 92631-2271478464	standard-read	standard-write-owner	standard-write-dac
MsSecCore	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532 92631-2271478464	standard-delete	query-service-config	change-service-config
MsSecCore	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532 92631-2271478464	query-service-status	enumerate-service-de pendents	start-service
MsSecCore	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532 92631-2271478464	stop-service	pause-continue-service	-
MsSecCore	Access Allowed for S-1-5-80-956008885-3418 522649-1831038044-18532 92631-2271478464	generic-all	-	-
MsSecCore	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
MsSecCore	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
MsSecCore	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
MsSecCore	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
MsSecCore	Access Allowed for Administrators	query-service-config	change-service-config	query-service-status
MsSecCore	Access Allowed for Administrators	enumerate-service-de pendents	start-service	stop-service
MsSecCore	Access Allowed for Administrators	pause-continue-service	nterrogate-service	-
MsSecCore	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
MsSecCore	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
MsSecCore	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
MsSecCore	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

MsSecCore	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
MsSecCore	Access Allowed for Service_Logon	service-user-defined-control	-	-
mssmbios	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
mssmbios	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
mssmbios	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
mssmbios	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
mssmbios	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
mssmbios	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
mssmbios	Access Allowed for Administrators	stop-service	pause-continue-service	-
mssmbios	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
mssmbios	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
mssmbios	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
mssmbios	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Mup	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Mup	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Mup	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Mup	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Mup	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Mup	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Mup	Access Allowed for Administrators	stop-service	pause-continue-service	-
Mup	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Mup	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Mup	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Mup	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NDIS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NDIS	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NDIS	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NDIS	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NDIS	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NDIS	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
NDIS	Access Allowed for Administrators	stop-service	pause-continue-service	-
NDIS	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NDIS	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NDIS	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status

NDIS	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NdisCap	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NdisCap	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NdisCap	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NdisCap	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NdisCap	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NdisCap	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
NdisCap	Access Allowed for Administrators	stop-service	pause-continue-service	-
NdisCap	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NdisCap	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NdisCap	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NdisCap	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NdisVirtualBus	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NdisVirtualBus	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NdisVirtualBus	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NdisVirtualBus	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NdisVirtualBus	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NdisVirtualBus	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
NdisVirtualBus	Access Allowed for Administrators	stop-service	pause-continue-service	-
NdisVirtualBus	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NdisVirtualBus	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NdisVirtualBus	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NdisVirtualBus	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Ndu	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Ndu	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Ndu	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Ndu	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Ndu	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Ndu	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Ndu	Access Allowed for Administrators	stop-service	pause-continue-service	-
Ndu	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Ndu	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Ndu	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Ndu	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

NetBIOS	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NetBIOS	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NetBIOS	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NetBIOS	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NetBIOS	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NetBIOS	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
NetBIOS	Access Allowed for Administrators	stop-service	pause-continue-service	-
NetBIOS	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
NetBIOS	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NetBIOS	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
NetBIOS	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NetBT	Access Allowed for Authenticated_Users	standard-read	query-service-config	query-service-status
NetBT	Access Allowed for Authenticated_Users	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
NetBT	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
NetBT	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
NetBT	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
NetBT	Access Allowed for Administrators	stop-service	pause-continue-service	-
NetBT	Access Allowed for System_Operators	standard-read	query-service-config	query-service-status
NetBT	Access Allowed for System_Operators	enumerate-service-de pendents	start-service	stop-service
NetBT	Access Allowed for System_Operators	pause-continue-service	nterrogate-service	service-user-defined-control
NetBT	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
NetBT	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
NetBT	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
NetBT	Access Allowed for Local_Service	pause-continue-service	-	-
NetBT	Access Allowed for Network_Service	pause-continue-service	-	-
NetBT	Access Allowed for Network_Configuration_O perators	standard-read	query-service-config	query-service-status
NetBT	Access Allowed for Network_Configuration_O perators	enumerate-service-de pendents	start-service	nterrogate-service
NetBT	Access Allowed for Network_Configuration_O perators	service-user-defined-control	-	-
Npfs	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Npfs	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Npfs	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Npfs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Npfs	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config

Npfs	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Npfs	Access Allowed for Administrators	stop-service	pause-continue-service	-
Npfs	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Npfs	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Npfs	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Npfs	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
npsvctrig	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
npsvctrig	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
npsvctrig	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
npsvctrig	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
npsvctrig	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
npsvctrig	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
npsvctrig	Access Allowed for Administrators	stop-service	pause-continue-service	-
npsvctrig	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
npsvctrig	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
npsvctrig	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
npsvctrig	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
nsiproxy	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
nsiproxy	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
nsiproxy	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
nsiproxy	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
nsiproxy	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
nsiproxy	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
nsiproxy	Access Allowed for Administrators	stop-service	pause-continue-service	-
nsiproxy	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
nsiproxy	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
nsiproxy	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
nsiproxy	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Ntfs	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Ntfs	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Ntfs	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Ntfs	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Ntfs	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Ntfs	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service

Ntfs	Access Allowed for Administrators	stop-service	pause-continue-service	-
Ntfs	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Ntfs	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Ntfs	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Ntfs	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Null	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Null	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Null	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Null	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Null	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Null	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Null	Access Allowed for Administrators	stop-service	pause-continue-service	-
Null	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Null	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Null	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Null	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
partmgr	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
partmgr	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
partmgr	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
partmgr	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
partmgr	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
partmgr	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
partmgr	Access Allowed for Administrators	stop-service	pause-continue-service	-
partmgr	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
partmgr	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
partmgr	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
partmgr	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
pci	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
pci	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
pci	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
pci	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
pci	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
pci	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
pci	Access Allowed for Administrators	stop-service	pause-continue-service	-

pci	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
pci	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
pci	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
pci	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
pcw	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
pcw	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
pcw	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
pcw	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
pcw	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
pcw	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
pcw	Access Allowed for Administrators	stop-service	pause-continue-service	-
pcw	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
pcw	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
pcw	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
pcw	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
pdc	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
pdc	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
pdc	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
pdc	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
pdc	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
pdc	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
pdc	Access Allowed for Administrators	stop-service	pause-continue-service	-
pdc	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
pdc	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
pdc	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
pdc	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
PEAUTH	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
PEAUTH	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
PEAUTH	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
PEAUTH	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
PEAUTH	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
PEAUTH	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
PEAUTH	Access Allowed for Administrators	stop-service	pause-continue-service	-
PEAUTH	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status

PEAUTH	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
PEAUTH	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
PEAUTH	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Psched	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Psched	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
Psched	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
Psched	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
Psched	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
Psched	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
Psched	Access Allowed for Administrators	stop-service	pause-continue-service	-
Psched	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
Psched	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
Psched	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
Psched	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
rdbss	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
rdbss	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
rdbss	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
rdbss	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
rdbss	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
rdbss	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
rdbss	Access Allowed for Administrators	stop-service	pause-continue-service	-
rdbss	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
rdbss	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
rdbss	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
rdbss	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
rdpbus	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
rdpbus	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
rdpbus	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
rdpbus	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
rdpbus	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
rdpbus	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
rdpbus	Access Allowed for Administrators	stop-service	pause-continue-service	-
rdpbus	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
rdpbus	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

rdpbus	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
rdpbus	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
rdyboost	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
rdyboost	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
rdyboost	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
rdyboost	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
rdyboost	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
rdyboost	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
rdyboost	Access Allowed for Administrators	stop-service	pause-continue-service	-
rdyboost	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
rdyboost	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
rdyboost	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
rdyboost	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
rspndr	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
rspndr	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
rspndr	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
rspndr	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
rspndr	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
rspndr	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
rspndr	Access Allowed for Administrators	stop-service	pause-continue-service	-
rspndr	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
rspndr	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
rspndr	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
rspndr	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
SgrmAgent	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	standard-read	standard-write-owner	standard-write-dac
SgrmAgent	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	standard-delete	query-service-config	change-service-config
SgrmAgent	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	query-service-status	enumerate-service-dependents	start-service
SgrmAgent	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	stop-service	pause-continue-service	-
SgrmAgent	Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464	generic-all	-	-
SgrmAgent	Access Allowed for Local_System	standard-read	query-service-config	query-service-status

SgrmAgent	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
SgrmAgent	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
SgrmAgent	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
SgrmAgent	Access Allowed for Administrators	query-service-config	change-service-config	query-service-status
SgrmAgent	Access Allowed for Administrators	enumerate-service-de pendents	start-service	stop-service
SgrmAgent	Access Allowed for Administrators	pause-continue-service	nterrogate-service	-
SgrmAgent	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
SgrmAgent	Access Allowed for Interactive_Logon	enumerate-service-de pendents	start-service	nterrogate-service
SgrmAgent	Access Allowed for Interactive_Logon	service-user-defined-control	-	-
SgrmAgent	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
SgrmAgent	Access Allowed for Service_Logon	enumerate-service-de pendents	start-service	nterrogate-service
SgrmAgent	Access Allowed for Service_Logon	service-user-defined-control	-	-
spaceport	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
spaceport	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
spaceport	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
spaceport	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
spaceport	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
spaceport	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
spaceport	Access Allowed for Administrators	stop-service	pause-continue-service	-
spaceport	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
spaceport	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
spaceport	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
spaceport	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
srv2	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
srv2	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
srv2	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
srv2	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
srv2	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
srv2	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
srv2	Access Allowed for Administrators	stop-service	pause-continue-service	-
srv2	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
srv2	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
srv2	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
srv2	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control

srvnet	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
srvnet	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
srvnet	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
srvnet	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
srvnet	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
srvnet	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
srvnet	Access Allowed for Administrators	stop-service	pause-continue-service	-
srvnet	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
srvnet	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
srvnet	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
srvnet	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
storahci	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
storahci	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
storahci	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
storahci	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
storahci	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
storahci	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
storahci	Access Allowed for Administrators	stop-service	pause-continue-service	-
storahci	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
storahci	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
storahci	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
storahci	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
storqosflt	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
storqosflt	Access Allowed for Local_System	enumerate-service-de pendents	start-service	stop-service
storqosflt	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
storqosflt	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
storqosflt	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
storqosflt	Access Allowed for Administrators	query-service-status	enumerate-service-de pendents	start-service
storqosflt	Access Allowed for Administrators	stop-service	pause-continue-service	-
storqosflt	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
storqosflt	Access Allowed for Interactive_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
storqosflt	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
storqosflt	Access Allowed for Service_Logon	enumerate-service-de pendents	nterrogate-service	service-user-defined-control
swenum	Access Allowed for Local_System	standard-read	query-service-config	query-service-status

swenum	Access Allowed for Local_System	enumerate-service-dependents	start-service	stop-service
swenum	Access Allowed for Local_System	pause-continue-service	nterrogate-service	service-user-defined-control
swenum	Access Allowed for Administrators	standard-read	standard-write-owner	standard-write-dac
swenum	Access Allowed for Administrators	standard-delete	query-service-config	change-service-config
swenum	Access Allowed for Administrators	query-service-status	enumerate-service-dependents	start-service
swenum	Access Allowed for Administrators	stop-service	pause-continue-service	-
swenum	Access Allowed for Interactive_Logon	standard-read	query-service-config	query-service-status
swenum	Access Allowed for Interactive_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
swenum	Access Allowed for Service_Logon	standard-read	query-service-config	query-service-status
swenum	Access Allowed for Service_Logon	enumerate-service-dependents	nterrogate-service	service-user-defined-control
Tcpip	Access Allowed for Local_System	standard-read	query-service-config	query-service-status
Results were truncated.				

 2 Microsoft Windows Effective Permission on Shares Enumerated

QID:	105185
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/25/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Detected effective security permissions for shares on the target host are enumerated, the complete set of effective permissions might differ.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	SHARE TYPE	ACE TYPE	NAME	PRIMARY GROUP	ACE1	ACE2	ACE3	ADDITIONAL INFO
ADMIN$	Hidden Directory	Access Allowed for Group	NT SERVICE\TrustedInstaller	NT SERVICE\TrustedInstaller	generic-all	standard-read	standard-write-owner	-

ADMIN$	Hidden Directory	Access Allowed for Group	NT SERVICE\TrustedInstaller	NT SERVICE\TrustedInstaller	standard-write-dac	standard-delete	-	-
ADMIN$	Hidden Directory	Access Allowed for Group	Local_System	NT SERVICE\TrustedInstaller	generic-all	standard-read	standard-delete	-
ADMIN$	Hidden Directory	Access Allowed for Group	Administrators	NT SERVICE\TrustedInstaller	generic-all	standard-read	standard-delete	-
ADMIN$	Hidden Directory	Access Allowed for Group	Users	NT SERVICE\TrustedInstaller	generic-read	generic-execute	standard-read	-
ADMIN$	Hidden Directory	Access Allowed for Group	Creator_Owner	NT SERVICE\TrustedInstaller	generic-all	-	-	-
ADMIN$	Hidden Directory	Access Allowed for Group	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	NT SERVICE\TrustedInstaller	generic-read	generic-execute	standard-read	-
ADMIN$	Hidden Directory	Access Allowed for Group	APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	NT SERVICE\TrustedInstaller	generic-read	generic-execute	standard-read	-
C$	Hidden Directory	Access Allowed for Group	Administrators	NT SERVICE\TrustedInstaller	standard-read	standard-write-owner	standard-write-dac	-
C$	Hidden Directory	Access Allowed for Group	Administrators	NT SERVICE\TrustedInstaller	standard-delete	-	-	-
C$	Hidden Directory	Access Allowed for Group	Local_System	NT SERVICE\TrustedInstaller	standard-read	standard-write-owner	standard-write-dac	-
C$	Hidden Directory	Access Allowed for Group	Local_System	NT SERVICE\TrustedInstaller	standard-delete	-	-	-
C$	Hidden Directory	Access Allowed for Group	Users	NT SERVICE\TrustedInstaller	standard-read	-	-	-
C$	Hidden Directory	Access Allowed for Group	Authenticated_Users	NT SERVICE\TrustedInstaller	generic-read	generic-write	generic-execute	-
C$	Hidden Directory	Access Allowed for Group	Authenticated_Users	NT SERVICE\TrustedInstaller	standard-delete	-	-	-

2 Microsoft Windows Hardening - Service Configuration

QID:	105187
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The service configuration for each win32 service, including the service startup type and service account name, is enumerated.

Turning off non-essential services is an important step in hardening a Windows system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Starttype	AccountName
AllJoyn Router Service	Manual	NT AUTHORITY\LocalService
Application Layer Gateway Service	Manual	NT AUTHORITY\LocalService
Application Identity	Manual	NT Authority\LocalService
Application Information	Manual	LocalSystem
Application Management	Manual	LocalSystem
App Readiness	Manual	LocalSystem
Microsoft App-V Client	Disabled	LocalSystem
AppX Deployment Service (AppXSVC)	Manual	LocalSystem
AssignedAccessManager Service	Manual	LocalSystem
Windows Audio Endpoint Builder	Automatic	LocalSystem
Windows Audio	Automatic	NT AUTHORITY\LocalService
Cellular Time	Manual	NT AUTHORITY\LocalService
ActiveX Installer (AxInstSV)	Manual	LocalSystem
BitLocker Drive Encryption Service	Manual	localSystem
Base Filtering Engine	Automatic	NT AUTHORITY\LocalService
Background Intelligent Transfer Service	Manual	LocalSystem
Background Tasks Infrastructure Service	Automatic	LocalSystem
Bluetooth Audio Gateway Service	Manual	NT AUTHORITY\LocalService
AVCTP service	Manual	NT AUTHORITY\LocalService
Bluetooth Support Service	Manual	NT AUTHORITY\LocalService
Capability Access Manager Service	Manual	LocalSystem
Connected Devices Platform Service	Automatic	NT AUTHORITY\LocalService
Certificate Propagation	Manual	LocalSystem
Client License Service (ClipSVC)	Manual	LocalSystem
Microsoft Cloud Identity Service	Manual	NT AUTHORITY\NetworkService
COM+ System Application	Manual	LocalSystem
CoreMessaging	Automatic	NT AUTHORITY\LocalService
Cryptographic Services	Automatic	NT Authority\NetworkService
Offline Files	Manual	LocalSystem
DCOM Server Process Launcher	Automatic	LocalSystem
dcsvc	Manual	LocalSystem
Optimize drives	Manual	localSystem
Device Association Service	Automatic	LocalSystem
Device Install Service	Manual	LocalSystem
DevQuery Background Discovery Broker	Manual	LocalSystem

DHCP Client	Automatic	NT Authority\LocalService
Microsoft (R) Diagnostics Hub Standard Collector Service	Manual	LocalSystem
Diagnostic Execution Service	Manual	LocalSystem
Connected User Experiences and Telemetry	Automatic	LocalSystem
DialogBlockingService	Disabled	LocalSystem
Display Policy Service	Automatic	NT AUTHORITY\LocalService
Display Enhancement Service	Manual	LocalSystem
Device Management Enrollment Service	Manual	LocalSystem
Device Management Wireless Application Protocol (WAP) Push message Routing Service	Manual	LocalSystem
DNS Client	Automatic	NT AUTHORITY\NetworkService
Delivery Optimization	Automatic	NT Authority\NetworkService
Wired AutoConfig	Manual	localSystem
Diagnostic Policy Service	Automatic	NT AUTHORITY\LocalService
Device Setup Manager	Manual	LocalSystem
Data Sharing Service	Manual	LocalSystem
Data Usage	Automatic	NT Authority\LocalService
Extensible Authentication Protocol	Manual	localSystem
Microsoft Edge Update Service (edgeupdate)	Automatic	LocalSystem
Microsoft Edge Update Service (edgeupdatem)	Manual	LocalSystem
Encrypting File System (EFS)	Manual	LocalSystem
Embedded Mode	Manual	LocalSystem
Enterprise App Management Service	Manual	LocalSystem
Windows Event Log	Automatic	NT AUTHORITY\LocalService
COM+ Event System	Automatic	NT AUTHORITY\LocalService
Fax	Manual	NT AUTHORITY\NetworkService
Function Discovery Provider Host	Manual	NT AUTHORITY\LocalService
Function Discovery Resource Publication	Manual	NT AUTHORITY\LocalService
File History Service	Manual	LocalSystem
Windows Font Cache Service	Automatic	NT AUTHORITY\LocalService
Windows Camera Frame Server	Manual	LocalSystem
GameInput Service	Manual	LocalSystem
Group Policy Client	Automatic	LocalSystem
GraphicsPerfSvc	Manual	LocalSystem
Human Interface Device Service	Manual	LocalSystem
HV Host Service	Manual	LocalSystem
Windows Mobile Hotspot Service	Manual	NT Authority\LocalService
IKE and AuthIP IPsec Keying Modules	Automatic	LocalSystem
Microsoft Store Install Service	Manual	LocalSystem
IP Helper	Automatic	LocalSystem
IP Translation Configuration Service	Manual	LocalSystem
CNG Key Isolation	Manual	LocalSystem
KtmRm for Distributed Transaction Coordinator	Manual	NT AUTHORITY\NetworkService
Server	Automatic	LocalSystem
Workstation	Automatic	NT AUTHORITY\NetworkService
Geolocation Service	Manual	LocalSystem
Windows License Manager Service	Manual	NT Authority\LocalService
Link-Layer Topology Discovery Mapper	Manual	NT AUTHORITY\LocalService
TCP/IP NetBIOS Helper	Manual	NT AUTHORITY\LocalService
Local Session Manager	Automatic	LocalSystem
Language Experience Service	Manual	LocalSystem
Downloaded Maps Manager	Automatic	NT AUTHORITY\NetworkService
McpManagementService	Manual	LocalSystem
Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)	Manual	LocalSystem
Windows Mixed Reality OpenXR Service	Manual	LocalSystem
Windows Defender Firewall	Automatic	NT Authority\LocalService

Distributed Transaction Coordinator	Manual	NT AUTHORITY\NetworkService
Microsoft iSCSI Initiator Service	Manual	LocalSystem
Windows Installer	Manual	LocalSystem
Microsoft Keyboard Filter	Disabled	LocalSystem
Natural Authentication	Manual	LocalSystem
Network Connectivity Assistant	Manual	LocalSystem
Network Connection Broker	Manual	LocalSystem
Network Connected Devices Auto-Setup	Manual	NT AUTHORITY\LocalService
Netlogon	Manual	LocalSystem
Network Connections	Manual	LocalSystem
Network List Service	Manual	NT AUTHORITY\LocalService
Network Setup Service	Manual	LocalSystem
Net.Tcp Port Sharing Service	Disabled	NT AUTHORITY\LocalService
Microsoft Passport Container	Manual	NT AUTHORITY\LocalService
Microsoft Passport	Manual	LocalSystem
Network Location Awareness	Automatic	NT AUTHORITY\NetworkService
Network Store Interface Service	Automatic	NT Authority\LocalService
Peer Networking Identity Manager	Manual	NT AUTHORITY\LocalService
Peer Networking Grouping	Manual	NT AUTHORITY\LocalService
Program Compatibility Assistant Service	Manual	LocalSystem
BranchCache	Manual	NT AUTHORITY\NetworkService
Windows Perception Simulation Service	Manual	LocalSystem
Performance Counter DLL Host	Manual	NT AUTHORITY\LocalService
Phone Service	Manual	NT Authority\LocalService
Performance Logs & Alerts	Manual	NT AUTHORITY\LocalService
Plug and Play	Manual	LocalSystem
PNRP Machine Name Publication Service	Manual	NT AUTHORITY\LocalService
Peer Name Resolution Protocol	Manual	NT AUTHORITY\LocalService
IPsec Policy Agent	Manual	NT Authority\NetworkService
Power	Automatic	LocalSystem
Printer Extensions and Notifications	Manual	LocalSystem
User Profile Service	Automatic	LocalSystem
Windows PushToInstall Service	Manual	LocalSystem
Quality Windows Audio Video Experience	Manual	NT AUTHORITY\LocalService
Remote Access Auto Connection Manager	Manual	localSystem
Remote Access Connection Manager	Manual	localSystem
Routing and Remote Access	Disabled	localSystem
Remote Registry	Automatic	NT AUTHORITY\LocalService
Retail Demo Service	Manual	LocalSystem
Radio Management Service	Manual	NT AUTHORITY\LocalService
RPC Endpoint Mapper	Automatic	NT AUTHORITY\NetworkService
Remote Procedure Call (RPC) Locator	Manual	NT AUTHORITY\NetworkService
Remote Procedure Call (RPC)	Automatic	NT AUTHORITY\NetworkService
Security Accounts Manager	Automatic	LocalSystem
Smart Card	Manual	NT AUTHORITY\LocalService
Smart Card Device Enumeration Service	Manual	LocalSystem
Task Scheduler	Automatic	LocalSystem
Smart Card Removal Policy	Manual	LocalSystem
Windows Backup	Manual	localSystem
Secondary Logon	Manual	LocalSystem
Windows Security Service	Manual	LocalSystem
Payments and NFC/SE Manager	Manual	NT AUTHORITY\LocalService
System Event Notification Service	Automatic	LocalSystem
Windows Defender Advanced Threat Protection Service	Manual	LocalSystem
Sensor Data Service	Manual	LocalSystem

Sensor Service	Manual	LocalSystem
Sensor Monitoring Service	Manual	NT AUTHORITY\LocalService
Remote Desktop Configuration	Manual	localSystem
System Guard Runtime Monitor Broker	Automatic	LocalSystem
Internet Connection Sharing (ICS)	Manual	LocalSystem
Spatial Data Service	Manual	NT AUTHORITY\LocalService
Shell Hardware Detection	Automatic	LocalSystem
Shared PC Account Manager	Disabled	LocalSystem
Microsoft Storage Spaces SMP	Manual	NT AUTHORITY\NetworkService
Microsoft Windows SMS Router Service.	Manual	NT Authority\LocalService
SNMP Trap	Manual	NT AUTHORITY\LocalService
Windows Perception Service	Manual	NT AUTHORITY\LocalService
Print Spooler	Automatic	LocalSystem
Software Protection	Automatic	NT AUTHORITY\NetworkService
SSDP Discovery	Manual	NT AUTHORITY\LocalService
OpenSSH Authentication Agent	Disabled	LocalSystem
Secure Socket Tunneling Protocol Service	Manual	NT Authority\LocalService
State Repository Service	Manual	LocalSystem
Windows Image Acquisition (WIA)	Manual	NT Authority\LocalService
Storage Service	Automatic	LocalSystem
Spot Verifier	Manual	LocalSystem
Microsoft Software Shadow Copy Provider	Manual	LocalSystem
SysMain	Automatic	LocalSystem
System Events Broker	Automatic	LocalSystem
Touch Keyboard and Handwriting Panel Service	Manual	LocalSystem
Telephony	Manual	NT AUTHORITY\NetworkService
Remote Desktop Services	Manual	NT Authority\NetworkService
Themes	Automatic	LocalSystem
Storage Tiers Management	Manual	localSystem
Time Broker	Manual	NT AUTHORITY\LocalService
Web Account Manager	Manual	LocalSystem
Distributed Link Tracking Client	Automatic	LocalSystem
Recommended Troubleshooting Service	Manual	LocalSystem
Windows Modules Installer	Manual	localSystem
Auto Time Zone Updater	Disabled	NT AUTHORITY\LocalService
User Experience Virtualization Service	Disabled	LocalSystem
Remote Desktop Services UserMode Port Redirector	Manual	localSystem
UPnP Device Host	Manual	NT AUTHORITY\LocalService
User Manager	Automatic	LocalSystem
Update Orchestrator Service	Automatic	LocalSystem
Volumetric Audio Compositor Service	Manual	NT AUTHORITY\LocalService
Credential Manager	Manual	LocalSystem
VirtualBox Guest Additions Service	Automatic	LocalSystem
Virtual Disk	Manual	LocalSystem
Hyper-V Guest Service Interface	Manual	LocalSystem
Hyper-V Heartbeat Service	Manual	LocalSystem
Hyper-V Data Exchange Service	Manual	LocalSystem
Hyper-V Remote Desktop Virtualization Service	Manual	LocalSystem
Hyper-V Guest Shutdown Service	Manual	LocalSystem
Hyper-V Time Synchronization Service	Manual	NT AUTHORITY\LocalService
Hyper-V PowerShell Direct Service	Manual	LocalSystem
Hyper-V Volume Shadow Copy Requestor	Manual	LocalSystem
Volume Shadow Copy	Manual	LocalSystem
Windows Time	Manual	NT AUTHORITY\LocalService
Windows Update Medic Service	Manual	LocalSystem

WalletService	Manual	LocalSystem
WarpJITSvc	Manual	NT Authority\LocalService
Block Level Backup Engine Service	Manual	localSystem
Windows Biometric Service	Manual	LocalSystem
Windows Connection Manager	Automatic	NT Authority\LocalService
Windows Connect Now - Config Registrar	Manual	NT AUTHORITY\LocalService
Diagnostic Service Host	Manual	NT AUTHORITY\LocalService
Diagnostic System Host	Manual	LocalSystem
Microsoft Defender Antivirus Network Inspection Service	Manual	NT AUTHORITY\LocalService
WebClient	Manual	NT AUTHORITY\LocalService
Windows Event Collector	Manual	NT AUTHORITY\NetworkService
Windows Encryption Provider Host Service	Manual	NT AUTHORITY\LocalService
Problem Reports Control Panel Support	Manual	localSystem
Windows Error Reporting Service	Manual	localSystem
Wi-Fi Direct Services Connection Manager Service	Manual	NT AUTHORITY\LocalService
Still Image Acquisition Events	Manual	LocalSystem
Microsoft Defender Antivirus Service	Automatic	LocalSystem
WinHTTP Web Proxy Auto-Discovery Service	Manual	NT AUTHORITY\LocalService
Windows Management Instrumentation	Automatic	localSystem
Windows Remote Management (WS-Management)	Manual	NT AUTHORITY\NetworkService
Windows Insider Service	Manual	LocalSystem
WLAN AutoConfig	Manual	LocalSystem
Microsoft Account Sign-in Assistant	Manual	LocalSystem
Local Profile Assistant Service	Manual	NT Authority\LocalService
Windows Management Service	Manual	LocalSystem
WMI Performance Adapter	Manual	localSystem
Windows Media Player Network Sharing Service	Manual	NT AUTHORITY\NetworkService
Work Folders	Manual	NT AUTHORITY\LocalService
Parental Controls	Manual	LocalSystem
Portable Device Enumerator Service	Manual	LocalSystem
Windows Push Notifications System Service	Automatic	LocalSystem
Security Center	Automatic	NT AUTHORITY\LocalService
Windows Search	Automatic	LocalSystem
Windows Update	Manual	LocalSystem
WWAN AutoConfig	Manual	localSystem
Xbox Live Auth Manager	Manual	LocalSystem
Xbox Live Game Save	Manual	LocalSystem
Xbox Accessory Management Service	Manual	LocalSystem
Xbox Live Networking Service	Manual	LocalSystem
Mozilla Maintenance Service	Manual	LocalSystem
Agent Activation Runtime 5bb811	Manual	
GameDVR and Broadcast User Service 5bb811	Manual	
Bluetooth User Support Service 5bb811	Manual	
CaptureService 5bb811	Manual	
Clipboard User Service 5bb811	Manual	
Connected Devices Platform User Service 5bb811	Automatic	
ConsentUX 5bb811	Manual	
CredentialEnrollmentManagerUserSvc 5bb811	Manual	
DeviceAssociationBroker 5bb811	Manual	
DevicePicker 5bb811	Manual	
DevicesFlow 5bb811	Manual	
MessagingService 5bb811	Manual	
Sync Host 5bb811	Automatic	
Contact Data 5bb811	Manual	
PrintWorkflow 5bb811	Manual	

Udk User Service 5bb811	Manual
User Data Storage 5bb811	Manual
User Data Access 5bb811	Manual
Windows Push Notifications User Service 5bb811	Automatic

 2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot

QID:	105188
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Permissions for critical system files and folders are enumerated. Keeping these files and folders secure is critical for keeping the system secure.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: SOX
Section: N/A
Description: All critical network segments and those network segments containing servers/equipment performing production process/support of Sarbanes applications/data are protected by proven and tested firewalls at all network entry points.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

---------- ---------- --		
%windir%		
---------- ---------- --		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data

			read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\AppPatch			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\debug			
---------- ---------- --			
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	object_inherit container_inherit	
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --		
%windir%\Help		
---------- ---------- --		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --		
%windir%\inf		
---------- ---------- --		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

%windir%\installer			
---------- ---------- --			
SYSTEM	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Everyone	access_allowed	object_inherit container_inherit	synchronize standard_read execute read_data read_attributes read_extended_attributes
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%windir%\media			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\Registration			
---------- ---------- --			
Administrators	access_allowed	object_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Everyone	access_allowed	object_inherit	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	object_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data

			read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%windir%\security			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\Temp			
---------- ---------- --			
Users	access_allowed	container_inherit	synchronize append_data execute write_data
Administrators	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%ProgramFiles%\Common Files			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data

		read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

2 Microsoft Windows Folder Permission Check - Folders Under System32

QID:	105189
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The permissions of critical folders under the System32 directory are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

---------- ---------- --		
%windir%\System32		
---------- ---------- --		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\System32\ias			
---------- ---------- --			
Administrators	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
NETWORK_SERVICE	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes read_extended_attributes
SYSTEM	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%windir%\System32\Config			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed	container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data

			read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%windir%\System32\spool\printers			
---------- ---------- --			
Users	access_allowed	container_inherit	synchronize append_data write_data read_attributes read_extended_attributes
SYSTEM	access_allowed		standard_write_dac synchronize append_data standard_read standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
---------- ---------- --			
%windir%\System32\LogFiles			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%windir%\System32\inetsrv			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

SYSTEM	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

2 Microsoft Windows File Security Check - C: System Files

QID:	105190
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/13/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The security permissions for system files which are located on C: (primary partition drive) are enumerated. It is important that these files are properly secured.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: HIPAA
Section: 164.308(a)(ii)(D)
Description: Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

Type: SOX
Section: N/A
Description: Every user has a confidential password for access into a Company's system resources. These passwords are:
1) Changed frequently, as all individual users are automatically required to change their passwords
2) The display and printing of passwords is masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

c:\			
---------- ---------- --			
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed	object_inherit container_inherit	synchronize standard_read execute read_data read_attributes read_extended_attributes
Authenticated_Users	access_allowed		append_data
---------- ---------- --			
%ProgramFiles%			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Administrators	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --			
%CommonProgramFiles%			
---------- ---------- --			
NT SERVICE\TrustedInstaller	access_allowed		standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
SYSTEM	access_allowed		synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes

Administrators	access_allowed	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

2 Microsoft Windows Folder Security - Folders Under Document and Settings

QID:	105191
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The permissions of common folders under the Document and Settings folder are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%userprofile%\Default User

SYSTEM	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes

			delete_child standard_delete read_extended_attributes
Users	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
Everyone	access_allowed		synchronize standard_read execute read_data read_attributes read_extended_attributes
---------- ---------- --------			
%userprofile%\All Users			
---------- ---------- --------			
SYSTEM	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	object_inherit container_inherit	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed	object_inherit container_inherit	synchronize append_data standard_read execute write_data write_extended_attributes read_data read_attributes write_attributes read_extended_attributes

2 Security Permissions for Important CIFS Pipes

QID:	105244
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/29/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The security permissions for important operating system created named pipes are enumerated from the target Microsoft Windows system.

IMPACT:

Critical system interfaces are exposed through several CIFS pipes. Insecure permission settings can aid unauthorized access.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

\SAMR

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Administrators access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\eventlog

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
NT SERVICE\EventLog access_allowed append_data standard_read read_data read_attributes read_extended_attributes write_data
Owner_Rights access_allowed read_data

\winreg

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
NT SERVICE\BthAvctpSvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\bthserv access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\CaptureService access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\CDPSvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\DispBrokerDesktopSvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\EventSystem access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\fdPHost access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\FontCache access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\LicenseManager access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\lltdsvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\netprofm access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\nsi access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\PhoneSvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\RemoteRegistry access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\SharedRealitySvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\SstpSvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\tzautoupdate access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\WdiServiceHost access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\WebClient access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NT SERVICE\workfolderssvc access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
Owner_Rights access_allowed standard_read

\srvsvc

AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
SYSTEM access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\lsass

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Administrators access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\spoolss

Users access_allowed read_data write_data
Everyone access_allowed write_attributes read_attributes standard_read execute read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes read_attributes standard_read execute read_data write_extended_attributes read_extended_attributes write_data
Creator_Owner access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
SYSTEM access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
Administrators access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\svcctl

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Administrators access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\wkssvc

AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
SYSTEM access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
NETWORK_SERVICE access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data
---
\NETLOGON

Everyone access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
AnonymousLogon access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed write_attributes standard_read read_attributes read_data write_extended_attributes read_extended_attributes write_data
Administrators access_allowed standard_write_dac standard_delete read_data delete_child read_extended_attributes read_attributes append_data standard_read execute write_attributes standard_write_owner write_extended_attributes write_data


2 Last Successful User Login

QID:	105311
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/21/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The last successful user login was able to be determined. Refer to the Results section of this QID for details.

IMPACT:

Please make sure this finding is in compliance with your company's security policy.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastLoggedOnUser = .\User
LastLoggedOnSAMUser = .\User
LastLoggedOnProvider = {60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}

2 Microsoft Windows Permission on Shares Enumerated

QID:	105335
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/03/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Security permissions for shares on the target host are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

share	SHARE TYPE	ACE TYPE	NAME	OWNER	ACE1	ACE2	ACE3
ADMIN$	Hidden_Directory	No_Explicit_DACLS	-	-	-	-	-
C$	Hidden_Directory	No_Explicit_DACLS	-	-	-	-	-
IPC$	Hidden_IPC	No_Explicit_DACLS	-	-	-	-	-

2 Antivirus Information Extracted Using WMI for Windows Desktop

QID: 105591

Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Name and status of the antivirus software (enabled/disabled, uptodate/notuptodate) is extracted on the windows host using wmi wql queries.

NOTE: This QID supports only Vista and later released non server Windows operating systems.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Windows Defender	Enabled	up-to-date	397568

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
10.0.0.197	No registered hostname

1 Network Adapter MAC Address

QID:	43007
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

It is possible to obtain the MAC address information of the network adapters on the target system. Various sources such as SNMP and NetBIOS provide such information. This vulnerability test attempts to gather and report on this information in a table format.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Method	MAC Address	Vendor		
NBTSTAT	08:00:27:F6:69:EE	CADMUS COMPUTER SYSTEMS		
#table	cols="5"			
DESCRIPTION	IP ADDRESS	MAC ADDRESS	Default IP Gateway	Subnet Mask
Intel(R) PRO/1000 MT Desktop Adapter	10.0.0.197 fe80::641e:149e:4486:57a1	08:00:27:F6:69:EE	10.0.0.1	255.255.255.0 64

1 Processor Information for Windows Target System

QID:	43113
Category:	Hardware

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/13/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Processor information for the Windows target host is shown in the Result section.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Control\Session Manager\Environment		
PROCESSOR_IDENTIFIER	=	Intel64 Family 6 Model 142 Stepping 10, GenuineIntel
HKLM\System\CurrentControlSet\Control\Session Manager\Environment		
PROCESSOR_ARCHITECTURE	=	AMD64
HKLM\System\CurrentControlSet\Control\Session Manager\Environment		
PROCESSOR_LEVEL	=	6
HKLM\System\CurrentControlSet\Control\Session Manager\Environment		
NUMBER_OF_PROCESSORS	=	1
HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0		
ProcessorNameString	=	Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz

1 Processor And BIOS Information Overview On Windows

QID:	43567
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/21/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Information about the Windows's processor and BIOS is enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Control \Session Manager\Environment		
PROCESSOR_IDENTIFIER	=	Intel64 Family 6 Model 142 Stepping 10, GenuineIntel
HKLM\SYSTEM\CurrentControlSet\Control \SystemInformation		
BIOSVersion	=	VirtualBox
BIOSReleaseDate	=	12/01/2006
SystemManufacturer	=	innotek GmbH
SystemProductName	=	VirtualBox
InformationSource	=	0
ComputerHardwareIds	=	{4729b95a-7ba3-5f84-81c6-c5ade245ca5b}, {8b5b2632-fd4e-5683-b703-7aa8f7a67e7b}, {f4af0e4f-b6b1-51e6-b1b0-e89122ff97c2}, {d115e295-974b-5e75-9adc-d977e762cf4b}, {d85b4471-f11d-5da8-9969-7418961197e5}, {5036187d-2671-5cd8-8843-4719dfd33c5e}, {d14a935a-d678-579f-8875-3aab3d456c85}
ComputerHardwareId	=	{df037cfb-6deb-5b17-aa71-67af033ccb01}
HKLM\SYSTEM\CurrentControlSet\Control \SystemInformation		

1 Processor Microcode Revision Information Overview On Windows

QID:	43576
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/11/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Information about the Windows's Processor Microcode Revision is enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Hardware\Description\System\CentralProcessor\0		
Identifier	=	Intel64 Family 6 Model 142 Stepping 10
HKLM\Hardware\Description\System\CentralProcessor\0		
Update Revision	=	0000000000000000
HKLM\Hardware\Description\System\CentralProcessor\0		
Previous Update Revision	=	0000000000000000

1 Chassis Type of Systems Information for Windows

QID:	43733
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

chassis type of systems Information for the Windows target host is shown in the Result section.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Manufacturer: Oracle Corporation
SerialNumber:
ChassisTypes: Other

1 Disabled Accounts Enumerated From SAM Database

QID:	45027
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/23/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Security Accounts Manager holds user and machine account information. The scanner found at least one disabled user or machine account in the

SAM database for the target Windows machine. The accounts found are listed in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Disabled User/Machine Accounts:
Administrator
DefaultAccount
Guest
WDAGUtilityAccount

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 276 seconds

Start time: Mon, Sep 23 2024, 16:06:42 GMT

End time: Mon, Sep 23 2024, 16:11:18 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
DESKTOP-LN5HE01	NTLM DNS
DESKTOP-LN5HE01	NTLM NetBIOS
DESKTOP-LN5HE01	NetBIOS
DESKTOP-LN5HE01	Computer name

1 NTFS Settings Enumerated

QID:	45063
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/26/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NTFS settings on the target have been enumerated.

IMPACT:

n/a

SOLUTION:

For information on the significance of some of these settings, see this Microsoft TechNet article (http://www.microsoft.com/technet/scriptcenter/guide/sas_fsd_xdvz.mspx?mfr=true) and this article (http://www.tweakxp.com/article37043.aspx) published by a third party.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Filesystem
NtfsDisable8dot3NameCreation = 2
HKLM\SYSTEM\CurrentControlSet\Control\Filesystem
NtfsDisableLastAccessUpdate = 2147483650
HKLM\SYSTEM\CurrentControlSet\Control\Filesystem
Win31FileSystem = 0

1 Interface Names and Assigned IP Address Enumerated from Registry

QID:	45099
Category:	Information gathering

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Interface names and IP addresses assigned to those interfaces are listed for Windows 2000 and later versions of Microsoft Windows Operating

system. This test obtains this list by querying the registry database.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Interface:	Intel(R) PRO/1000 MT Desktop Adapter	IP Address:	10.0.0.197
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{174DEAEC-B50B-4C73-8732-EA3E61744353}			
EnableDHCP	=	0	
Domain	=		
NameServer	=	1.1.1.1	
DhcpServer	=	255.255.255.255	
SubnetMask	=	{"255.255.255.0"}	
DefaultGateway	=	{"10.0.0.1"}	

1 Mozilla Firefox Web Browser Detected

QID:	45108
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/09/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Mozilla Firefox is a free and open source web browser descended from the Mozilla Application Suite and managed by Mozilla Corporation.

An instance of Firefox was detected on the target.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
HKLM\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox CurrentVersion = 104.0 (x86 en-US)

1 Microsoft Windows Management Instrumentation Service (WMI) Is Running

QID:	45183
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/04/2012
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

The target has WMI service installed and running.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

winmgmt = RUNNING

1 Internet Protocol version 6 (IPv6) Enabled on Target Host

QID:	45193
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/08/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that routes traffic across the Internet. It is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013.

This QID uses the registry key mentioned in Microsoft KB929852 (http://support.microsoft.com/kb/929852) to determine if IPv6 is enabled.

The detection works in the following way:
1) For Windows 2000,XP,2003
-- Check for existence of key "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters"
2) For Windows Vista or 2008 or Windows 7 or Windows 8 or Windows Server 2012 and Windows RT:
-- It checks the value of "DisabledComponents" for key "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters"
Note: This checks make use of Windows Management Instrumentation(WMI) to list IPv6 Addresses on target.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

fe80::641e:149e:4486:57a1

1 System and BaseBoard Serial Numbers

QID:	45208
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The system serial number and baseboard serial number of the target device are reported in the Result section.

Requirements for Windows Operating Systems: This QID requires the Windows Management Instrumentation (WMI) service to be running. For the system serial number, the result is obtained through a WQL query on the "SerialNumber" Property of the "Win32_BIOS" WMI Class. For the baseboard serial number, the result is obtained through a WQL query on the "SerialNumber" Property of the "Win32_BaseBoard" WMI Class.

Requirements for Solaris Operating Systems: This QID requires the "smbios" or "sneep" command to be present on the system. The output of the result is the System Serial Number and Base Board Serial Number of the remote Solaris machine. If a remote Solaris machine only has the "sneep" command, then just System Serial Number will be posted.

Requirements for Linux Operating Systems: This QID requires "lshal" or "dmidecode" to be installed on the target. The result section lists the System Serial Number and Base Board Serial Number provided by "lshal" or "dmidecode".

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

System Serial Number : VirtualBox-b5349a4d-078c-401d-ad96-9cd80e4760f1
BaseBoard Serial Number : 0

1 Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430)

QID:	45225
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	KB2813430, KB2677070
Bugtraq ID:	-
Service Modified:	08/11/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

An automatic updater of revoked certificates (that is, either KB 2677070 or KB 2813430) is installed. An automatic updater of revoked certificates is available for Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. This updater expands on the existing automatic root update mechanism technology that is found in Windows Vista and in Windows 7 to let certificates that are compromised, or are untrusted in some way, be specifically flagged as untrusted.

Note: An automatic updater of revoked certificates is included in supported editions of Windows 8, Windows 8.1, Windows RT, Windows RT 8.1, Windows Server 2012, and Windows Server 2012 R2 Operating systems.

IMPACT:

Customers who have this update installed will benefit from quick automatic updates of untrusted certificates.

SOLUTION:

For more information please refer to Microsoft knowledge base KB2813430 (http://support.microsoft.com/kb/2813430) and KB2677070

(http://support.microsoft.com/kb/2677070).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate DisallowedCertLastSyncTime exists.

1 Trusted Digital Certificates Enumerated From Windows Registry

QID:	45231
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The results section of this QID contains the Digitial Certificates trusted by the system.
Note: The list is enumerated from the registry.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate	Issuer	Subject	Serial Number	Valid From (MM/DD/YY)	Expires (MM/DD/YY)
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	0ce7e0e517d846fe8fe560fc1bf03039	11/10/2006	11/10/2031
51501FBFCE69189D609CFAF140C576755DCC1FDF	Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	0cb30f70f286a433e0b90989de01edb7	12/08/2013	12/08/2043
73A5E64A3BFF8316FF0EDCCC618A906E4EAE4D74	Microsoft RSA Root Certificate Authority 2017	Microsoft RSA Root Certificate Authority 2017	1ed397095fd8b4b347701eaabe7f45b3	12/18/2019	07/18/2042
742C3192E607E424EB4549542BE1BBC53E6174E2	Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification Authority	70bae41d10d92934b638ca7b03ccbabf	01/29/1996	08/01/2028
7E04DE896A3E666D00E687D33FFAD93BE83D349E	DigiCert Global Root G3	DigiCert Global Root G3	055556bcf25ea43535c3a40fd5ab4572	08/01/2013	01/15/2038

	DigiCert Global Root CA	DigiCert Global Root CA	083be056904246b1a1756ac95991c74a	11/10/2006	11/10/2031
B1BC968BD4F49D622AA89A81F2150152A41D829C	GlobalSign Root CA	GlobalSign Root CA	040000000001154b5ac394	09/01/1998	01/28/2028
CABD2A79A1076A31F21D253635CB039D4329A5E8	ISRG Root X1	ISRG Root X1	8210cfb0d240e3594463e0bb63828b00	06/04/2015	06/04/2035
DF3C24F9BFD666761B268073FE06D1CC8D4F82A4	DigiCert Global Root G2	DigiCert Global Root G2	033af1e6a711a9a0bbb2864b11d09fae5	08/01/2013	01/15/2038
109F1CAED645BB78B3EA2B94C0697C740733031C	Microsoft Root Authority	Microsoft Windows Hardware Compatibility	198b11d13f9a8ffe69a0	10/01/1997	12/31/2002
D559A586669B08F46A30A133F8A9ED3D038E2EA8	Class 3 Public Primary Certification Authority	"VeriSign, Inc.", VeriSign International Server CA - Class 3, www.verisign.com/ CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign	46fcebbab4d02f0f926098233f93078f	04/17/1997	10/24/2016
FEE449EE0E3965A5246F000E87FDE2A065FD89D4	Root Agency	Root Agency	06376c00aa00648a11cfb8d4aa5c35f4	05/28/1996	12/31/2039
0119E81BE9A14CD8E22F40AC118C687ECBA3F4D8	Microsoft Time Stamp Root Certificate Authority 2014	Microsoft Time Stamp Root Certificate Authority 2014	2fd67a432293329045e953343ee27466	10/22/2014	10/22/2039
06F1AA330B927B753A40E68CDF22E34BCBEF3352	Microsoft ECC Product Root Certificate Authority 2018	Microsoft ECC Product Root Certificate Authority 2018	14982666dc7ccd8f4053677bb999ec85	02/27/2018	02/27/2043
18F7C1FCC3090203FD5BAA2F861A754976C8DD25	"VeriSign, Inc.", VeriSign Time Stamping Service Root, "NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc."	"VeriSign, Inc.", VeriSign Time Stamping Service Root, "NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc."	4a19d2388c82591ca55d735f155ddca3	05/12/1997	01/07/2004
245C97DF7514E7CF2DF8BE72AE957B9E04741E85	Microsoft Corporation, Microsoft Time Stamping Service Root, Copyright (c) 1997 Microsoft Corp.	Microsoft Corporation, Microsoft Time Stamping Service Root, Copyright (c) 1997 Microsoft Corp.	01	05/13/1997	12/30/1999
31F9FC8BA3805986B721EA7295C65B3A44534274	Microsoft ECC TS Root Certificate Authority 2018	Microsoft ECC TS Root Certificate Authority 2018	153875e1647ed1b047b4efaf41128245	02/27/2018	02/27/2043
3B1EFD3A66EA28B16697394703A72CA340A05BD5	Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	28cc3a25bfba44ac449a9b586b4339aa	06/23/2010	06/23/2035
4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	18dad19e267de8bb4a2158cdcc6b3b4a	11/08/2006	07/16/2036
7F88CD7223F3C813818C994614A89C99FA3B5247	Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	01	01/01/1995	12/31/1999
8F43288AD272F3103B6FB1428485EA3014C0BCFE	Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authority 2011	3f8bc8b5fc9fb29643b569d66c42e144	03/22/2011	03/22/2036
92B46C76E13054E104F230517E6E504D43AB10B5	Symantec Enterprise Mobile Root for Microsoft	Symantec Enterprise Mobile Root for Microsoft	0f6b552f9ebf907b0f6629a9bdf4d8ce	03/15/2012	03/14/2032
A43489159A520F0D93D032CCAF37E7FE20A8B419	Microsoft Root Authority	Microsoft Root Authority	c1008b3c3c8811d13ef663ecdf40	01/10/1997	12/31/2020
BE36A4562FB2EE05DBB3D32323ADF445084ED656	Thawte Timestamping CA	Thawte Timestamping CA	00	01/01/1997	12/31/2020
CDD4EEAE6000AC7F40C3802C171E30148030C072	Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	79ad16a14aa0a5ad4c7358f407132e65	05/09/2001	05/09/2021

	DigiCert Trusted Root G4	DigiCert Trusted Root G4	059b1b579e8e2132e23907bda777755c	08/01/2013	01/15/2038

1 Network Interface Information Extracted Through WMI

QID:	45232
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Interface name, IP address and MAC address information is extracted on the remote system using wmi wql queries.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESCRIPTION	IP ADDRESS	MAC ADDRESS	Default IP Gateway	Subnet Mask
Intel(R) PRO/1000 MT Desktop Adapter	10.0.0.197 fe80::641e:149e:4486:57a1	08:00:27:F6:69:EE	10.0.0.1	255.255.255.0 64

1 PowerShell Detected On Host

QID:	45254
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/07/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

PowerShell (including Windows PowerShell and PowerShell Core) is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework. PowerShell was made open-source and cross-platform (Windows, Linux, and macOS) on 18 August 2016.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine PowerShellVersion = 2.0
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe found
HKLM\SOFTWARE\Microsoft\PowerShell\3\PowerShellEngine PowerShellVersion = 5.1.19041.1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe found
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\PowerShellEngine PowerShellVersion = 2.0
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe found
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\3\PowerShellEngine PowerShellVersion = 5.1.19041.1
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe found

 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/22/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:

N/A

SOLUTION:

For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SMB Version 2 detected on TCP port 445.
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters SMB2 is missing.
SMB Server version 2 or 3 is Enabled
HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb20 Start = 3
SMB Client version 2 or 3 is Enabled

1 McAfee Data Loss Prevention Endpoint Agent not Installed

QID:	45272
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

McAfee Data Loss Prevention (DLP) Endpoint safeguards intellectual property and ensures compliance by protecting sensitive data on endpoint systems.

The target does not have McAfee Data Loss Prevention Endpoint Agent installed on it.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\McAfee\DLP\Agent is missing
HKLM\SOFTWARE\Wow6432Node\McAfee\DLP\Agent is missing
McAfee DLP Agent Missing on Target

1 Microsoft Edge Installed on Windows.

QID:	45291
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/04/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Edge (codename "Spartan") is a web browser developed by Microsoft and included in Windows 10, Windows Server 2016, Windows 10 Mobile and Xbox One, replacing Internet Explorer as the default web browser on all device classes.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe found
Microsoft Edge Installed
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.52

1 System Management BIOS UUID Detected

QID:	45303
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/05/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The system management BIOS UUID is reported in the Result section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Windows SMBIOS UUID : B5349A4D-078C-401D-AD96-9CD80E4760F1

1 Windows Boot Method Detected

QID:	45309
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/30/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The result section contains the boot method for this windows system (UEFI Mode or legacy BIOS mode).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Boot Method: BIOS Detected
HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot\State is missing

1 Microsoft Windows 10 Operating System Detected

QID:	45342
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/16/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows 10 is a series of personal computer operating systems produced by Microsoft as part of its Windows NT family of operating systems. It is the successor to Windows 8.1, and was released to manufacturing on July 15, 2015, and became generally available on July 29, 2015

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows NT\CurrentVersion
ProductName = Windows 10 Pro
ReleaseId = 2009

 1 Windows/Linux/Unix Hostname Information

QID:	45361
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/12/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

QID will collect the hostname from Windows/LINUX/UNIX Machines.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HOSTNAME: DESKTOP-LN5HE01

1 Report TimeZone Information

QID:	45366
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

QID will collect the TimeZone information from Machines.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
TimeZoneKeyName = Eastern Standard Time
UTC = -04:00

1 Microsoft Windows Network Level Authentication Enabled

QID:	45379
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/10/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Windows Network Level Authentication (NLA) is an authentication method that enhances the security of a Remote Desktop Session Host server by requiring the user to be authenticated before a session is created.

The registry key for the Network Level Authentication (NLA) is Enabled.
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication (0 = Disabled | 1 = Enabled)

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services UserAuthentication is missing.
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp UserAuthentication = 1
Microsoft Windows Network Level Authentication Enabled

 1 Status of Remote Desktop/Terminal Service

QID:	45381
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Desktop Services (RDS), also known as Terminal Services is one of the components of Microsoft Windows that allow a user to take control of a remote computer or virtual machine over a network connection.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TermService is STOPPED NT Authority\NetworkService

1 Installed Locale settings on Host

QID:	45382
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/30/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The locale settings installed on the host is identified as in the results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

LANG=en_US

1 Windows Running Service Permissions

QID:	45414
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The QID list prints out the permissions for executables related to running Services on a Windows host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\\Windows\\system32\\svchost.exe		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
C:\\Windows\\System32\\svchost.exe		
NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
C:\\Program Files (x86)\\Microsoft\\EdgeUpdate\\MicrosoftEdgeUpdate.exe		
SYSTEM	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\lsass.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\fxssvc.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\GameInputSvc.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\lsass.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\ 129.0.2792.52\\elevation_service.exe		

S-1-15-3-1024-3424233489-972189580-2057154623-747635277-1604371224-316187997-3786583170-1043257646	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
S-1-15-3-1024-2302894289-466761758-1166120688-1039016420-2430351297-4240214049-4028510897-3317428798	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\msdtc.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\msiexec.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\Microsoft.NET\\Framework 64\\v4.0.30319\\SMSvcHost.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\PerceptionSimulation\\PerceptionSimulationService.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\SysWow64\\perfhost.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\alg.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\AppVClient.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\dllhost.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\DiagSvcs\\DiagnosticsHub.StandardCollector.Service.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\locator.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\SecurityHealthService.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files\\Windows Defender Advanced Threat Protection\\MsSense.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\SensorDataService.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\SgrmBroker.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\snmptrap.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\spectrum.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\spoolsv.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\sppsvc.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\OpenSSH\\ssh-agent.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\TieringEngineService.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\servicing\\TrustedInstaller.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\AgentService.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\VBoxService.exe		

SYSTEM	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\System32\\vds.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\vssvc.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\wbengine.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files\\Windows Defender\\NisSrv.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files\\Windows Defender\\MsMpEng.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

---		
C:\\Windows\\system32\\wbem\\WmiApSrv.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files\\Windows Media Player\\wmpnetwk.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Windows\\system32\\SearchIndexer.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
---		
C:\\Program Files (x86)\\Mozilla Maintenance Service\\maintenanceservice.exe		

SYSTEM	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
----------		
C:\\Windows\\system32\\CredentialEnrollmentManager.exe		

NT SERVICE\TrustedInstaller	access_allowed	standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
Administrators	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
SYSTEM	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
Users	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES	access_allowed	synchronize standard_read execute read_data read_attributes read_extended_attributes

1 Microsoft Windows ScForceOption Registry Key Detected

QID:	45425
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Windows ScForceOption Registry Key Detected on host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

scforceoption = 0
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System
scforceoption = 0

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:14
TCP	445	0:02:16
UDP	137	0:00:56
UDP	138	0:00:07
UDP	500	0:00:12
UDP	1900	0:00:12

1 Microsoft OneDrive Software Detected

QID:	45428
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/07/2020
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

Microsoft OneDrive Save your files and photos to OneDrive and access them from any device, anywhere.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%systemdrive%\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe Version is 21.220.1024.5

1 Microsoft Windows Fast Startup Feature Is Enabled

QID:	45445
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Windows Updates Not Install With Fast Startup
Bugtraq ID:	-
Service Modified:	06/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows updates might not be installed on your system after you shut down your computer. This behavior occurs when the Fast Startup feature is enabled. This behavior does not occur when you restart your computer.

IMPACT:

Updates may not be installed with Fast Startup

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Power HiberbootEnabled = 1

1 Current Logged in User Listed

QID:	45448
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The QID will check the current logged in User in Windows.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKCU\Volatile Environment USERNAME = User

1 Microsoft Windows Sense agent Detected

QID:	45453
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows Advanced Threat Protection is enabled on this host. This Qid will detect the status of Sense agent service and display information from HKLM\SOFTWARE\Microsoft\Windows Advanced Threat Protection and HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection registry keys.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Sense is STOPPED LocalSystem
Windows Defender Advanced Threat Protection 10.8675.25926.1031

 1 Microsoft Windows User Access Control Enabled

QID:	45454
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	UAC
Bugtraq ID:	-
Service Modified:	09/15/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

User Account Control is a mandatory access control enforcement facility introduced with Microsoft's Windows.

User Account Control (UAC) is a security component in Windows operating systems. UAC enables users to perform common tasks as non-administrators and as administrators without having to switch users, log off, or use Run As.

This QID checks for registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System to check if UAC is enable.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA = 1
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA = 1

1 Windows WMI AuthenticationLevel Status

QID:	45456
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Windows wmi authentication level
Bugtraq ID:	-
Service Modified:	09/04/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems. Winmgmt is the WMI service within the SVCHOST process running under the "LocalSystem" account.

The "level" argument in winmgmt /standalonehost is the authentication level for the Svchost process. WMI normally runs as part of a shared service host and you cannot increase the authentication level for WMI alone. If level is not specified, the default is 4 (RPC_C_AUTHN_LEVEL_PKT or WbemAuthenticationLevelPkt).

You can run WMI more securely by increasing the authentication level to Packet Privacy (Level 6) (RPC_C_AUTHN_LEVEL_PKT_PRIVACY or WbemAuthenticationLevelPktPrivacy).

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WMI AuthenticationLevel is not set or not accessible.

1 Windows Host Domain Role

QID:	45486
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/31/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Reports DomainRoles of Windows Host:
Standalone Workstation
Member Workstation
Standalone Server
Member Server
Backup Domain Controller
Primary Domain Controller

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DomainRole = Standalone Workstation

1 MultiThreading is Enabled

QID:	45489
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/05/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Report if MultiThreading is Enabled or Disabled

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Socket(s) : 1
Thread(s) per core : 1
NumberOfCores : 1
LogicalProcessors : 1
MultiThreading is Not Enabled

1 Windows Builtin User Group Membership Audit - Remote Desktop

QID:	45496
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/05/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

User accounts that are members of the remote desktop users group are enumerated from the target host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Desktop Users No members in this group

1 NetBIOS Over TCP/IP is enabled/disabled Status Detected

QID:	45497
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/21/2021
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

NetBIOS Over TCP/IP status Detected on the remote system using wmi wql queries.

**Note There are 3 status in NetBIOS setting
1. Default: (Numeric value 0)

2. Enable NetBIOS over TCP/IP(Numeric value 1)

3. Disable NetBIOS over TCP/IP(Numeric value 2)

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESCRIPTION	TCPIPNETBIOSOPTIONS
Intel(R) PRO/1000 MT Desktop Adapter	0

1 Microsoft Windows Print Spooler Service is running

QID:	45498
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/02/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This service spools print jobs and handles interaction with the printer.
NOTE: If you turn off this service, you will not be able to print or see

your printers.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Spooler = RUNNING

1 System Architecture Information for Windows and Unix Platform Detected

QID:	45501
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/05/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID checks the OS Architecture for Windows, Linux and MacOS

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment PROCESSOR_ARCHITECTURE = AMD64

1 Local Firewall Status on Windows Detected

QID:	45506
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/21/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Information about the Windows Defender Firewall is enumerated. The Result section lists true(1) in case firewall is ON-EnableFirewall=1 and false(0) in case of firewall is OFF-EnableFirewall=0.

The QID does not read the Windows Defender Firewall status set via Group Policy or Active Directory.

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile	EnableFirewall	=	1
Local Windows Firewall for Domain Profile is Enabled			
Local Windows Firewall for Public Profile is Disabled			
Local Windows Firewall for Standard Profile is Disabled			

1 Windows Running Processes

QID:	45517
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID shows detailed running processes for the Windows OS

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	CommandLine	Caption	CreationDate	Description	Executable Path	ExecutionState	InstallDate	ProcessId	TerminationDate
System Idle Process	N/A	System Idle Process	20240923111100.012597-240	System Idle Process	N/A	N/A	N/A	0	N/A
System	N/A	System	20240923111100.012597-240	System	N/A	N/A	N/A	4	N/A
Registry	N/A	Registry	20240923111058.519846-240	Registry	N/A	N/A	N/A	72	N/A
smss.exe	N/A	smss.exe	20240923111100.015086-240	smss.exe	N/A	N/A	N/A	340	N/A
csrss.exe	N/A	csrss.exe	20240923111106.249245-240	csrss.exe	N/A	N/A	N/A	432	N/A
wininit.exe	N/A	wininit.exe	20240923111106.501438-240	wininit.exe	N/A	N/A	N/A	500	N/A
services.exe	N/A	services.exe	20240923111106.604679-240	services.exe	N/A	N/A	N/A	592	N/A
lsass.exe	C:\Windows\system32\lsass.exe	lsass.exe	20240923111106.624086-240	lsass.exe	C:\Windows\system32\lsass.exe	N/A	N/A	600	N/A
fontdrvhost.exe	"fontdrvhost.exe"	fontdrvhost.exe	20240923111106.853211-240	fontdrvhost.exe	C:\Windows\system32\fontdrvhost.exe	N/A	N/A	732	N/A
VBoxService.exe	C:\Windows\System32\VBoxService.exe	VBoxService.exe	20240923111108.195635-240	VBoxService.exe	C:\Windows\System32\VBoxService.exe	N/A	N/A	1244	N/A
Memory Compression	N/A	Memory Compression	20240923111108.318931-240	Memory Compression	N/A	N/A	N/A	1316	N/A
spoolsv.exe	C:\Windows\System32\spoolsv.exe	spoolsv.exe	20240923111109.344296-240	spoolsv.exe	C:\Windows\System32\spoolsv.exe	N/A	N/A	1784	N/A
dasHost.exe	dashost.exe {ebd7c6fe-8916-41a6-b6740e037c011605}	dasHost.exe	20240923111110.464065-240	dasHost.exe	C:\Windows\system32\dashost.exe	N/A	N/A	2040	N/A
MsMpEng.exe	N/A	MsMpEng.exe	20240923111110.571498-240	MsMpEng.exe	N/A	N/A	N/A	1916	N/A
SearchIndexer.exe	C:\Windows\system32\SearchIndexer.exe /Embedding	SearchIndexer.exe	20240923111110.832274-240	SearchIndexer.exe	C:\Windows\system32\SearchIndexer.exe	N/A	N/A	2196	N/A
dasHost.exe	dashost.exe {10a0e829-61a4-4a54-a06e62223d6c9d2a}	dasHost.exe	20240923111111.013086-240	dasHost.exe	C:\Windows\system32\dashost.exe	N/A	N/A	2300	N/A
NisSrv.exe	N/A	NisSrv.exe	20240923111113.023746-240	NisSrv.exe	N/A	N/A	N/A	2588	N/A

	"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /c	MicrosoftEdgeUpdate.exe	20240923111117.068618-240	MicrosoftEdgeUpdate.exe	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	N/A	N/A	2948	N/A
SecurityHealthService.exe	N/A	SecurityHealthService.exe	20240923111143.626953-240	SecurityHealthService.exe	N/A	N/A	N/A	6604	N/A
SgrmBroker.exe	N/A	SgrmBroker.exe	20240923111310.920822-240	SgrmBroker.exe	N/A	N/A	N/A	7176	N/A
csrss.exe	N/A	csrss.exe	20240923115737.323069-240	csrss.exe	N/A	N/A	N/A	5032	N/A
winlogon.exe	winlogon.exe	winlogon.exe	20240923115737.368373-240	winlogon.exe	C:\Windows\system32\winlogon.exe	N/A	N/A	8636	N/A
dwm.exe	"dwm.exe"	dwm.exe	20240923115737.512385-240	dwm.exe	C:\Windows\system32\dwm.exe	N/A	N/A	6116	N/A
fontdrvhost.exe	"fontdrvhost.exe"	fontdrvhost.exe	20240923115737.566412-240	fontdrvhost.exe	C:\Windows\system32\fontdrvhost.exe	N/A	N/A	2072	N/A
sihost.exe	sihost.exe	sihost.exe	20240923115817.551348-240	sihost.exe	C:\Windows\system32\sihost.exe	N/A	N/A	5052	N/A
taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}	taskhostw.exe	20240923115817.774686-240	taskhostw.exe	C:\Windows\system32\taskhostw.exe	N/A	N/A	6716	N/A
explorer.exe	C:\Windows\Explorer.EXE	explorer.exe	20240923115818.769038-240	explorer.exe	C:\Windows\Explorer.EXE	N/A	N/A	7348	N/A
StartMenuExperienceHost.exe	"C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca	StartMenuExperienceHost.exe	20240923115821.956606-240	StartMenuExperienceHost.exe	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe	N/A	N/A	8384	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923115822.521540-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	1684	N/A
SearchApp.exe	"C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca	SearchApp.exe	20240923115823.678385-240	SearchApp.exe	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	N/A	N/A	1384	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923115824.277493-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	9104	N/A
ShellExperienceHost.exe	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t	ShellExperienceHost.exe	20240923115828.908972-240	ShellExperienceHost.exe	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	N/A	N/A	6400	N/A

	.mca								
ctfmon.exe	"ctfmon.exe"	ctfmon.exe	20240923115829.649969-240	ctfmon.exe	C:\Windows\system32\ctfmon.exe	N/A	N/A	2844	N/A
SkypeApp.exe	"C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeApp.exe" -ServerName:App.AppXffn3yxqvgawq9fpmnhy90fr3y01d1t5b.mca	SkypeApp.exe	20240923115829.664605-240	SkypeApp.exe	C:\Program FilesWindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeApp.exe	N/A	N/A	5240	N/A
SkypeBackgroundHost.exe	"C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe" -ServerName:SkypeBackgroundHost	SkypeBackgroundHost.exe	20240923115829.764485-240	SkypeBackgroundHost.exe	C:\Program FilesWindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe	N/A	N/A	5764	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923115833.718272-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	9140	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923115835.883422-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	4068	N/A
SecurityHealthSystray.exe	"C:\Windows\System32\SecurityHealthSystray.exe"	SecurityHealthSystray.exe	20240923115839.747292-240	SecurityHealthSystray.exe	C:\Windows\System32\SecurityHealthSystray.exe	N/A	N/A	5740	N/A
VBoxTray.exe	"C:\Windows\System32\VBoxTray.exe"	VBoxTray.exe	20240923115840.344623-240	VBoxTray.exe	C:\Windows\System32\VBoxTray.exe	N/A	N/A	5852	N/A
OneDrive.exe	"C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	OneDrive.exe	20240923115840.857770-240	OneDrive.exe	C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe	N/A	N/A	2804	N/A
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start	msedge.exe	20240923115843.716795-240	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A	N/A	2216	N/A
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\User\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\User\AppData\Local	msedge.exe	20240923115844.419334-240	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A	N/A	8080	N/A

	\Microsoft\Edge\User Data\Crashpad" "--metrics-dir=C:\Users\User\AppData\Local\Microsoft\Edge\User Data" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=129.0.6668.59 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=129.0.2792.52 --initial-client-data=0x244, 0x248, 0x24c, 0x240, 0x254, 0x7fffc2438ee0, 0x7fffc2438eec, 0x7fffc2438ef8								
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --string-annotations=is-enterprise-managed=no --gpu-preferences=UAAAAAAAAADgAAAMAAAAAAAAAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAA --field-trial-handle=2148,i,2854405778230971768,9672820653365819663,262144 --variations-seed-version --mojo-platform-channel-handle=2144 /prefetch:2	msedge.exe	20240923115844.629526-240	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A	N/A	6504	N/A
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"	msedge.exe	20240923115844.802903-240	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.	N/A	N/A	5372	N/A

	--type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --string-annotations=is-enterprise-managed=no --field-trial-handle=1896,i,2854405778230971768,9672820653365819663,262144 --variations-seed-version --mojo-platform-channel-handle=2632 /prefetch:3				exe				
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --string-annotations=is-enterprise-managed=no --field-trial-handle=2240,i,2854405778230971768,9672820653365819663,262144 --variations-seed-version --mojo-platform-channel-handle=2832 /prefetch:8	msedge.exe	20240923115844.894524-240	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A	N/A	7880	N/A
ApplicationFrameHost.exe	C:\Windows\system32\ApplicationFrameHost.exe -Embedding	ApplicationFrameHost.exe	20240923115856.928170-240	ApplicationFrameHost.exe	C:\Windows\system32\ApplicationFrameHost.exe	N/A	N/A	3672	N/A
WinStore.App.exe	"C:\Program Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\WinStore.App.exe" -ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca	WinStore.App.exe	20240923115856.948846-240	WinStore.App.exe	C:\Program Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\WinStore.App.exe	N/A	N/A	3748	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923115858.022538-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	7056	N/A

	"C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -ServerName:microsoft.windows.immersivecontrolpanel	SystemSettings.exe	20240923115907.955183-240	SystemSettings.exe	C:\Windows\ImmersiveControlPanel\SystemSettings.exe	N/A	N/A	5360	N/A
UserOOBEBroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding	UserOOBEBroker.exe	20240923115908.674896-240	UserOOBEBroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe	N/A	N/A	1472	N/A
RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe	20240923120029.777897-240	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe	N/A	N/A	7924	N/A
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	WmiPrvSE.exe	20240923120718.576709-240	WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	N/A	N/A	4356	N/A
TrustedInstaller.exe	C:\Windows\servicing\TrustedInstaller.exe	TrustedInstaller.exe	20240923120726.542311-240	TrustedInstaller.exe	C:\Windows\servicing\TrustedInstaller.exe	N/A	N/A	2276	N/A
TiWorker.exe	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3745_none_7ded3f327ca60a41\TiWorker.exe -Embedding	TiWorker.exe	20240923120726.580823-240	TiWorker.exe	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3745_none_7ded3f327ca60a41\TiWorker.exe	N/A	N/A	916	N/A
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	WmiPrvSE.exe	20240923120745.941711-240	WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	N/A	N/A	912	N/A
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	svchost.exe	20240923111106.856615-240	svchost.exe	C:\Windows\system32\svchost.exe	N/A	N/A	740	N/A

1 Add/Remove Installed Software Registry Keys

QID:	45520
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/23/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The installed applications at the Windows host are listed, alongwith RegistryKey associated to it. This qid obtains this list by querying the registry keys corresponding to the Installer Database.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Display Name	Display Version	Registry Key
Mozilla Maintenance Service	104.0	HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\MozillaMaintenanceService
Oracle VirtualBox Guest Additions 7.1.0	7.1.0.164728	HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VirtualBox Guest Additions
Microsoft Edge	129.0.2792.52	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Edge
Microsoft Edge Update	1.3.195.19	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Edge Update
Microsoft Edge WebView2 Runtime	128.0.2739.79	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft EdgeWebView
Mozilla Firefox (x86 en-US)	104.0	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 104.0 (x86 en-US)
VLC media player 1.1.1	1.1.1	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\VLC media player

1 ntoskrnl.exe Version Detected

QID:	45521
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This is an Information gathering QID that displays ntoskrnl.exe versions currently running on a system. The ntoskrnl.exe (short for Windows NT operating system kernel executable), also known as kernel image, provides the kernel and executive layers of the Microsoft Windows NT kernel space, and is responsible for various system services such as hardware abstraction, process and memory management, thus making it a fundamental part of the system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ntoskrnl.exe Version 10.0.19041.3803

1 Windows Prefetcher Enabled

QID:	45560
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/21/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The prefetcher behavior is controlled by the Windows registry value "EnablePrefetcher" located in the following registry path: HKLM\System\CurrentControlSet\Control\Session\Manager\ Memory Management\ PrefetchParameters. The value for "EnablePrefetcher" can have one of the following values [1]:

Report when the value is non-zero, that is Not Disabled.

IMPACT:

N/A

SOLUTION:

Read the Contents of Registy, if it's 1,2 or 3
Enable prefetch using the following approach:

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
Name: EnablePrefetcher
Type: REG_DWORD
Value: 1 (1, 2 or 3)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters EnablePrefetcher = 3
Application launch and boot enabled (default)

1 Windows Active Processors

QID:	45561
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/20/2023

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Total Active Processors information for the Windows target host is shown in the Result section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Control\Session Manager\Environment

NUMBER_OF_PROCESSORS	=	1

1 Microsoft Windows Status of FIPS Algorithm Policy

QID:	45567
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	FipsAlgorithmPolicy
Bugtraq ID:	-
Service Modified:	03/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Federal Information Processing Standard (FIPS) 140 is a security implementation that is designed for certifying cryptographic software. Windows implements these certified algorithms to meet the requirements and standards for cryptographic modules for use by departments and agencies of the United States federal government.

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard. FIPS is based on Section 5131 of the Information Technology Management Reform Act of 1996. It defines the minimum security requirements for cryptographic modules in IT products.

IMPACT:

N/A

SOLUTION:

Customers are advised to refer to FipsAlgorithmPolicy (https://learn.microsoft.com/en-US/windows/security/threat-protection/fips-140-validation) for further details pertaining to this.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy
Enabled = 0
---

1 Last Logged on User of Administrator Group

QID:	45582
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The last successful user login was able to be determined which is a Member of the built-in Administrator Group from the target Microsoft Windows system.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User
HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastLoggedOnUser = .\User
LastLoggedOnSAMUser = .\User
LastLoggedOnProvider = {60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}

1 Qualys Cloud Agent Not Installed

QID:	45592

Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Qualys
Bugtraq ID:	-
Service Modified:	01/16/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Below mentioned operating system is supported by Qualys Cloud Agent and is not installed on your host. Qualys Cloud Agent is a single agent for real-time, global visibility and response.

Please see Cloud Agent Platform Availability Matrix (PAM) for list of supported operating systems:
https://success.qualys.com/support/s/article/000006675

Solution: Install Qualys Cloud Agent. Please refer to this article
https://docs.qualys.com/en/csam/latest/inventory/sensors/cloud_agent.htm

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Qualys Agent is not installed

1 Microsoft Windows Sense Service is Stopped Detected

QID:	45623
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID detects the status of Sense agent service when stopped and display information from HKLM\SOFTWARE\Microsoft\Windows Advanced Threat

Protection and HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection registry keys.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Sense = STOPPED

1 Windows Host Environment Variables Detected

QID:	48196
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Environment Variables Information for the Windows target host is shown in the Result section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\ControlSet001\Control\Session Manager\Environment
ComSpec = %SystemRoot%\system32\cmd.exe
DriverData = C:\Windows\System32\Drivers\DriverData
OS = Windows_NT
Path = %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
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

TEMP = %SystemRoot%\TEMP
TMP = %SystemRoot%\TEMP
USERNAME = SYSTEM
windir = %SystemRoot%
NUMBER_OF_PROCESSORS = 1
PROCESSOR_LEVEL = 6
PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 142 Stepping 10, GenuineIntel
PROCESSOR_REVISION = 8e0a
---

1 Windows Host Local Group and Their Respective Users Detected

QID:	48202
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The IG QID will extract all the local groups and their respective Users in windows machine by wmi querying.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GroupName	:	UserName
Access Control Assistance Operators	:	
Administrators	:	Administrator, User,
Backup Operators	:	
Cryptographic Operators	:	
Device Owners	:	
Distributed COM Users	:	
Event Log Readers	:	
Guests	:	Guest,
Hyper-V Administrators	:	
IIS_IUSRS	:	IUSR,
Network Configuration Operators	:	
Performance Log Users	:	
Performance Monitor Users	:	
Power Users	:	

Remote Desktop Users	:	
Remote Management Users	:	
Replicator	:	
System Managed Accounts Group	:	DefaultAccount,
Users	:	INTERACTIVE, Authenticated Users,

1 Windows Connected Printers Information Extracted Through WMI

QID: 48203
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/03/2022
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The IG QID will extract all Connected Printers information by querying wmi.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	PrinterState	PrinterStatus
OneNote	0	3
Microsoft XPS Document Writer	0	3
Microsoft Print to PDF	0	3
HC Office Printer	0	3
Fax	0	3

1 List of installed Microsoft Windows Store/AppX Software using HKLM Registry Key

QID: 48204
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/28/2024
User Modified: -
Edited: No

PCI Vuln: No

THREAT:

This QID enumerates the installed Windows Store/AppX Software from registry key.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

AppName	AppVersion	AppLocation
MS_AppStore_Microsoft.549981C3F5F10	1.1911.21713.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.549981C3F5F10_1.1911.21713.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.BingWeather	4.25.20211.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.BingWeather_4.25.20211.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.DesktopAppInstaller	2019.125.2243.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_2019.125.2243.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.GetHelp	10.1706.13331.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.GetHelp_10.1706.13331.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.Getstarted	8.2.22942.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Getstarted_8.2.22942.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.HEIFImageExtension	1.0.22742.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.HEIFImageExtension_1.0.22742.0_x64__8wekyb3d8bbwe\
MS_AppStore_Microsoft.Microsoft3DViewer	6.1908.2042.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_6.1908.2042.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.MicrosoftEdge.Stable	129.0.2792.52	C:\Program Files\WindowsApps\Microsoft.MicrosoftEdge.Stable_129.0.2792.52_neutral__8wekyb3d8bbwe\
MS_AppStore_Microsoft.MicrosoftOfficeHub	18.1903.1152.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.1903.1152.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.MicrosoftSolitaireCollection	4.4.8204.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_4.4.8204.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.MicrosoftStickyNotes	3.6.73.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MicrosoftStickyNotes_3.6.73.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.MixedReality.Portal	2000.19081.1301.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MixedReality.Portal_2000.19081.1301.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.MSPaint	2019.729.2301.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MSPaint_2019.729.2301.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.Office.OneNote	16001.12026.20112.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Office.OneNote_16001.12026.20112.0_neutral_~_8wekyb3d8bbwe\

MS_AppStore_Microsoft.People	2019.305.632.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.People_2019.305.632.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.ScreenSketch	2019.904.1644.0	C:\Program Files\WindowsApps\Microsoft.ScreenSketch_2019.904.1644.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.SkypeApp	14.53.77.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_neutral_~_kzf8qxf38zg5c\
MS_AppStore_Microsoft.StorePurchaseApp	11811.1001.1813.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.StorePurchaseApp_11811.1001.1813.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.VCLibs.140.00	14.0.27323.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.27323.0_x64__8wekyb3d8bbwe\
MS_AppStore_Microsoft.VP9VideoExtensions	1.0.22681.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe\
MS_AppStore_Microsoft.Wallet	2.4.18324.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Wallet_2.4.18324.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WebMediaExtensions	1.0.20875.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WebMediaExtensions_1.0.20875.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WebpImageExtension	1.0.22753.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WebpImageExtension_1.0.22753.0_x64__8wekyb3d8bbwe\
MS_AppStore_Microsoft.Windows.Photos	2019.19071.12548.0	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsAlarms	2019.807.41.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsAlarms_2019.807.41.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsCalculator	2020.1906.55.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsCalculator_2020.1906.55.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsCamera	2018.826.98.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsCamera_2018.826.98.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_microsoft.windowscommunicationsapps	16005.11629.20316.0	%SYSTEMDRIVE%\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11629.20316.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsFeedbackHub	2019.1111.2029.0	C:\Program Files\WindowsApps\Microsoft.WindowsFeedbackHub_2019.1111.2029.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsMaps	2019.716.2316.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsMaps_2019.716.2316.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsSoundRecorder	2019.716.2313.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsSoundRecorder_2019.716.2313.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.WindowsStore	11910.1002.513.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.WindowsStore_11910.1002.513.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.Xbox.TCUI	1.23.28002.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Xbox.TCUI_1.23.28002.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.XboxApp	48.49.31001.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.XboxApp_48.49.31001.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.XboxGameOverlay	1.46.11001.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.XboxGameOverlay_1.46.11001.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.XboxGamingOverlay	2.34.28001.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_2.34.28001.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.XboxIdentityProvider	12.50.6001.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.XboxIdentityProvider_12.50.6001.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.XboxSpeechToTextOverlay	1.17.29001.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.XboxSpeechToTextOverlay_1.17.29001.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.YourPhone	2019.430.2026.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.YourPhone_2019.430.2026.0_neutral_~_8wekyb3d8bbwe\

MS_AppStore_Microsoft.ZuneMusic	2019.19071.19011.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.ZuneMusic_2019.19071.19011.0_neutral_~_8wekyb3d8bbwe\
MS_AppStore_Microsoft.ZuneVideo	2019.19071.19011.0	%SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.ZuneVideo_2019.19071.19011.0_neutral_~_8wekyb3d8bbwe\

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.

The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	User
Domain	(none)
Authentication Scheme	NTLMSSP v2
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	Login credentials provided by user
CIFS Signing	default
Authentication Record	Win10 Credentials
CIFS Version	SMB v3.1.1

1 Windows Login User Information

QID:	70035
Category:	SMB / NETBIOS

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows user account used during the scan has the following properties:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User name:	User
Full name:	
Home directory:	
Home drive:	
Account description:	
Last logon:	Mon Sep 23 16:07:11 2024
Password last set:	Mon Sep 23 15:57:16 2024
Password must change:	Fri Dec 13 20:45:52 1901
Member of	
None	

1 Windows Authentication Method for User-Provided Credentials

QID:	70053
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed and successful with user-provided credentials. The Results section in your detailed results includes a list of authentication credentials used.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	User
Domain	(none)
Authentication Scheme	NTLMSSP v2
Security	User-based
SMBv1 Signing	Disabled
Authentication Record	Win10 Credentials

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
500	isakmp	isakmp	unknown
1900	unknown	unknown	unknown

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	SMBv2	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	16:06:43 GMT
Unreachable (type=3 code=3)	UDP Port 1037	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3801	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6969	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 40422	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 1034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 17	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6670	Port Unreachable

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DESKTOP-LN5HE01

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1171905628 with a standard deviation of 695038063. These TCP initial sequence

numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5438 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 6 milli seconds

1 NetBIOS Workgroup Name Detected

QID:	82062
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/02/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS workgroup or domain name for this system has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WORKGROUP

1 Enabled Display Last Username

QID:	90008
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/13/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

By default, Windows NT logon displays the name of the last user logged on to the host. This feature is activated on this host.

IMPACT:

Unauthorized users with physical access to the host can use this information in an attempt to guess the login password.

SOLUTION:

We recommend disabling this automatic feature. To do so, locate the following registry key, and then create or set a REG_SZ 'DontDisplayLastUserName' entry to '1':

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

The same can be achieved by creating a similar value-data tuple as above for the group-policy HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System registry key.

The latter (group policy setting) overrides the former (local setting).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System DontDisplayLastUserName = 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon DontDisplayLastUserName is missing.

1 Enabled Shutdown Without Logon

QID:	90009
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/28/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

By default, Windows NT allows anyone with physical access to the
host to shut down the system, even if no one is logged on.

IMPACT:

Unauthorized users with physical access to the server can perform a shutdown,
including users without an account on the host.

SOLUTION:

We recommend disabling this feature, and limiting shutdown permissions for the server to local users with a login on this server. To do this, locate the following registry key, and then set the REG_DWORD 'ShutdownWithoutLogon' entry to '0':

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

COMPLIANCE:

Type: HIPAA
Section: 164.310(a)(1)
Description: Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System ShutdownWithoutLogon = 1

1 Windows CDROM Autorun Enabled

QID:	90012
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Autorun is activated on this host. Windows Autorun enables programs located on CDs to be automatically launched when a CD is inserted in the CD-ROM drive.

If Autorun is enabled, it puts the machine into potential malaware risk or even virus infection. Mostly, viruses and worms are spread using the

windows AutoRun feature.

In the past, Sony rootkit issue exploited machines that had Autorun enabled to secretly infect them by digital rights management software after playing certain CDs. The Downadup/Conficker worm is known to have infected a lot of machines and the use of the Autoplay functionality has been one of the major attack vector and propagation method for the worm to spread.

IMPACT:

If the machine can be accessed physically, then viruses or trojan attack programs can be installed with little difficulty.

SOLUTION:

We recommend that you remove the Autorun functionality. To do this, locate the following registry key, and then set the 'Autorun' entry to '0':

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

To selectively disable specific Autorun features, change the "NoDriveTypeAutoRun" entry in one of the following registry key subkeys:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\

The value of the NoDriveTypeAutoRun registry entry determines which drive or drives the Autorun functionality will be disabled for. Settings for the NoDriveTypeAutoRun registry entry are listed below:

0x1 = Disables AutoPlay on drives of unknown type
0x4 = Disables AutoPlay on removable drives
0x8 = Disables AutoPlay on fixed drives
0x10 = Disables AutoPlay on network drives
0x20 = Disables AutoPlay on CD-ROM drives
0x40 = Disables AutoPlay on RAM disks
0x80 = Disables AutoPlay on drives of unknown type
0xFF = Disables AutoPlay on all kinds of drives

You may also disable the service by setting the group policy object (GPO).
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun

Detailed steps on disabling the Autorun functionality for different Windows platforms through various methods are available at Microsoft Knowledge Base Articles KB967715 (http://support.microsoft.com/kb/967715) and KB953252 (http://support.microsoft.com/kb/953252).

NOTE: This qid Checks for value of two registry keys so to avoid being flagged modify the value of both registry keys ("HKLM\System\CurrentControlSet\Services\CDRom AutoRun and
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Services\CDRom AutoRun = 1

1 Disabled Clear Page File

QID:	90013
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/28/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows does not clear or recreate the page file on this system.

IMPACT:

This vulnerability could pose a threat to security and cause a drop in performance. Sensitive information, such as passwords or usernames, can be retrieved.

SOLUTION:

We recommend forcing Windows to clear the page file when the system shuts down. To do this, locate the following registry key, and then set the REG_SZ key 'ClearPageFileAtShutdown' to '1':

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management ClearPageFileAtShutdown = 0

 1 Possible Log Recording Issues

QID:	90014
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/28/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Security Log might stop recording events when it is full.

IMPACT:

When the system's maximum log size is reached, security-related events will no longer be logged. No authorized or unauthorized activity will be recorded.

SOLUTION:

Administrators requiring total visibility of all access attempts may wish to enable the system crash on audit-fail. This will shutdown the system until the administrator logs in and purges the event log. To activate this feature, locate the following registry key, and then set the 'CrashOnAuditFail' entry to '1':

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Control\Lsa CrashOnAuditFail = 0

1 Enabled Caching of Dial-up Password Feature

QID:	90015
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/28/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows has a feature that enables the dial-up password to be saved and then be automatically provided during connection attempts. This feature has been activated on this system.

IMPACT:

Windows saves these passwords using very weak encryption. Therefore, unauthorized local users may be able to retreive passwords without much difficulty.

Since Windows automatically provides the saved dial-up password, unauthorized users with local access to this host can connect and dial the remote host without the password.

SOLUTION:

We recommend that you disable caching of the dial-up password. To do this, locate the following registry key, and then set the REG_DWORD 'DisableSavePassword' entry to '1':

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\System\CurrentControlSet\Services\Rasman\Parameters DisableSavePassword is missing.

1 Windows Services List

QID:	90065
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/27/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following Windows services were detected.

IMPACT:

N/A

SOLUTION:

Stop unnused services, and set them to "Disabled" in the Windows "Services" Control Panel.

COMPLIANCE:

Type: GLBA
Section: N/A
Description: Identify users who use network services and who require access to necessary service configurations and authentication parameters.

Type: SOX
Section: N/A
Description: Limiting System Services
Identify the following services and server function/usage:- Identify critical services open on the server (i.e., FTP, Telnet, SSH, SMTP, DNS, Finger, HTTP, POP3, Portmapper, NNTP, Samba, IMAP2, SNMP, HTTPS, NNTPS, IMAPS, POP3S, and MySQL)- Identify additional uses of the server that may cause vulnerabilities such as remote access methods for administration (i.e., PC Anywhere, radmin, VNC), NETBIOS, SQL Server databases, Terminal Services- Identify users who use network services and who have access to the necessary service configuration and authentication parameters

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Status	Description
AJRouter		AllJoyn Router Service
ALG		Application Layer Gateway Service
AppIDSvc		Application Identity
Appinfo	started	Application Information
AppMgmt		Application Management
AppReadiness		App Readiness
AppVClient		Microsoft App-V Client
AppXSvc		AppX Deployment Service (AppXSVC)
AssignedAccessManagerSvc		AssignedAccessManager Service
AudioEndpointBuilder	started	Windows Audio Endpoint Builder
Audiosrv	started	Windows Audio
autotimesvc		Cellular Time
AxInstSV		ActiveX Installer (AxInstSV)
BDESVC		BitLocker Drive Encryption Service
BFE	started	Base Filtering Engine
BITS		Background Intelligent Transfer Service
BrokerInfrastructure	started	Background Tasks Infrastructure Service
BTAGService		Bluetooth Audio Gateway Service
BthAvctpSvc	started	AVCTP service
bthserv		Bluetooth Support Service
camsvc		Capability Access Manager Service
CDPSvc	started	Connected Devices Platform Service
CertPropSvc		Certificate Propagation
ClipSVC		Client License Service (ClipSVC)
cloudidsvc		Microsoft Cloud Identity Service
COMSysApp		COM+ System Application
CoreMessagingRegistrar	started	CoreMessaging
CryptSvc	started	Cryptographic Services
CscService		Offline Files
DcomLaunch	started	DCOM Server Process Launcher
dcsvc		dcsvc
defragsvc		Optimize drives

DeviceAssociationService	started	Device Association Service
DeviceInstall		Device Install Service
DevQueryBroker		DevQuery Background Discovery Broker
Dhcp	started	DHCP Client
diagnosticshub.standardcollector.service		Microsoft (R) Diagnostics Hub Standard Collector Service
diagsvc		Diagnostic Execution Service
DiagTrack	started	Connected User Experiences and Telemetry
DialogBlockingService		DialogBlockingService
DispBrokerDesktopSvc	started	Display Policy Service
DisplayEnhancementService		Display Enhancement Service
DmEnrollmentSvc		Device Management Enrollment Service
dmwappushservice		Device Management Wireless Application Protocol (WAP) Push message Routing Service
Dnscache	started	DNS Client
DoSvc		Delivery Optimization
dot3svc		Wired AutoConfig
DPS	started	Diagnostic Policy Service
DsmSvc		Device Setup Manager
DsSvc		Data Sharing Service
DusmSvc	started	Data Usage
Eaphost		Extensible Authentication Protocol
edgeupdate		Microsoft Edge Update Service (edgeupdate)
edgeupdatem		Microsoft Edge Update Service (edgeupdatem)
EFS		Encrypting File System (EFS)
embeddedmode		Embedded Mode
EntAppSvc		Enterprise App Management Service
EventLog	started	Windows Event Log
EventSystem	started	COM+ Event System
Fax		Fax
fdPHost	started	Function Discovery Provider Host
FDResPub	started	Function Discovery Resource Publication
fhsvc		File History Service
FontCache	started	Windows Font Cache Service
FrameServer		Windows Camera Frame Server
GameInputSvc		GameInput Service
gpsvc	started	Group Policy Client
GraphicsPerfSvc		GraphicsPerfSvc
hidserv		Human Interface Device Service
HvHost		HV Host Service
icssvc		Windows Mobile Hotspot Service
IKEEXT	started	IKE and AuthIP IPsec Keying Modules
InstallService	started	Microsoft Store Install Service
iphlpsvc	started	IP Helper
IpxlatCfgSvc		IP Translation Configuration Service
KeyIso	started	CNG Key Isolation
KtmRm		KtmRm for Distributed Transaction Coordinator
LanmanServer	started	Server
LanmanWorkstation	started	Workstation
lfsvc	started	Geolocation Service
LicenseManager	started	Windows License Manager Service
lltdsvc		Link-Layer Topology Discovery Mapper
lmhosts	started	TCP/IP NetBIOS Helper
LSM	started	Local Session Manager
LxpSvc		Language Experience Service
MapsBroker		Downloaded Maps Manager
McpManagementService		McpManagementService

MicrosoftEdgeElevationService		Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)
MixedRealityOpenXRSvc		Windows Mixed Reality OpenXR Service
mpssvc	started	Windows Defender Firewall
MSDTC		Distributed Transaction Coordinator
MSiSCSI		Microsoft iSCSI Initiator Service
msiserver		Windows Installer
MsKeyboardFilter		Microsoft Keyboard Filter
NaturalAuthentication		Natural Authentication
NcaSvc		Network Connectivity Assistant
NcbService	started	Network Connection Broker
NcdAutoSetup	started	Network Connected Devices Auto-Setup
Netlogon		Netlogon
Netman	started	Network Connections
netprofm	started	Network List Service
NetSetupSvc		Network Setup Service
NetTcpPortSharing		Net.Tcp Port Sharing Service
NgcCtnrSvc		Microsoft Passport Container
NgcSvc		Microsoft Passport
NlaSvc	started	Network Location Awareness
nsi	started	Network Store Interface Service
p2pimsvc		Peer Networking Identity Manager
p2psvc		Peer Networking Grouping
PcaSvc	started	Program Compatibility Assistant Service
PeerDistSvc		BranchCache
perceptionsimulation		Windows Perception Simulation Service
PerfHost		Performance Counter DLL Host
PhoneSvc		Phone Service
pla		Performance Logs & Alerts
PlugPlay	started	Plug and Play
PNRPAutoReg		PNRP Machine Name Publication Service
PNRPsvc		Peer Name Resolution Protocol
PolicyAgent	started	IPsec Policy Agent
Power	started	Power
PrintNotify		Printer Extensions and Notifications
ProfSvc	started	User Profile Service
PushToInstall		Windows PushToInstall Service
QWAVE		Quality Windows Audio Video Experience
RasAuto		Remote Access Auto Connection Manager
RasMan		Remote Access Connection Manager
RemoteAccess		Routing and Remote Access
RemoteRegistry	started	Remote Registry
RetailDemo		Retail Demo Service
RmSvc	started	Radio Management Service
RpcEptMapper	started	RPC Endpoint Mapper
RpcLocator		Remote Procedure Call (RPC) Locator
RpcSs	started	Remote Procedure Call (RPC)
SamSs	started	Security Accounts Manager
SCardSvr		Smart Card
ScDeviceEnum		Smart Card Device Enumeration Service
Schedule	started	Task Scheduler
SCPolicySvc		Smart Card Removal Policy
SDRSVC		Windows Backup
seclogon		Secondary Logon
SecurityHealthService	started	Windows Security Service
SEMgrSvc	started	Payments and NFC/SE Manager

SENS	started	System Event Notification Service
Sense		Windows Defender Advanced Threat Protection Service
SensorDataService		Sensor Data Service
SensorService		Sensor Service
SensrSvc		Sensor Monitoring Service
SessionEnv		Remote Desktop Configuration
SgrmBroker	started	System Guard Runtime Monitor Broker
SharedAccess		Internet Connection Sharing (ICS)
SharedRealitySvc		Spatial Data Service
ShellHWDetection	started	Shell Hardware Detection
shpamsvc		Shared PC Account Manager
smphost		Microsoft Storage Spaces SMP
SmsRouter		Microsoft Windows SMS Router Service.
SNMPTRAP		SNMP Trap
spectrum		Windows Perception Service
Spooler	started	Print Spooler
sppsvc		Software Protection
SSDPSRV	started	SSDP Discovery
ssh-agent		OpenSSH Authentication Agent
SstpSvc		Secure Socket Tunneling Protocol Service
StateRepository	started	State Repository Service
stisvc		Windows Image Acquisition (WIA)
StorSvc	started	Storage Service
svsvc		Spot Verifier
swprv		Microsoft Software Shadow Copy Provider
SysMain	started	SysMain
SystemEventsBroker	started	System Events Broker
TabletInputService	started	Touch Keyboard and Handwriting Panel Service
TapiSrv		Telephony
TermService		Remote Desktop Services
Themes	started	Themes
TieringEngineService		Storage Tiers Management
TimeBrokerSvc	started	Time Broker
TokenBroker	started	Web Account Manager
TrkWks	started	Distributed Link Tracking Client
TroubleshootingSvc		Recommended Troubleshooting Service
TrustedInstaller		Windows Modules Installer
tzautoupdate		Auto Time Zone Updater
UevAgentService		User Experience Virtualization Service
UmRdpService		Remote Desktop Services UserMode Port Redirector
upnphost		UPnP Device Host
UserManager	started	User Manager
UsoSvc	started	Update Orchestrator Service
VacSvc		Volumetric Audio Compositor Service
VaultSvc	started	Credential Manager
VBoxService	started	VirtualBox Guest Additions Service
vds		Virtual Disk
vmicguestinterface		Hyper-V Guest Service Interface
vmicheartbeat		Hyper-V Heartbeat Service
vmickvpexchange		Hyper-V Data Exchange Service
vmicrdv		Hyper-V Remote Desktop Virtualization Service
vmicshutdown		Hyper-V Guest Shutdown Service
vmictimesync		Hyper-V Time Synchronization Service
vmicvmsession		Hyper-V PowerShell Direct Service
vmicvss		Hyper-V Volume Shadow Copy Requestor

VSS		Volume Shadow Copy
W32Time		Windows Time
WaaSMedicSvc	started	Windows Update Medic Service
WalletService		WalletService
WarpJITSvc		WarpJITSvc
wbengine		Block Level Backup Engine Service
WbioSrvc	started	Windows Biometric Service
Wcmsvc	started	Windows Connection Manager
wcncsvc		Windows Connect Now - Config Registrar
WdiServiceHost	started	Diagnostic Service Host
WdiSystemHost		Diagnostic System Host
WdNisSvc	started	Microsoft Defender Antivirus Network Inspection Service
WebClient		WebClient
Wecsvc		Windows Event Collector
WEPHOSTSVC		Windows Encryption Provider Host Service
wercplsupport		Problem Reports Control Panel Support
WerSvc		Windows Error Reporting Service
WFDSConMgrSvc		Wi-Fi Direct Services Connection Manager Service
WiaRpc		Still Image Acquisition Events
WinDefend	started	Microsoft Defender Antivirus Service
WinHttpAutoProxySvc	started	WinHTTP Web Proxy Auto-Discovery Service
Winmgmt	started	Windows Management Instrumentation
WinRM		Windows Remote Management (WS-Management)
wisvc		Windows Insider Service
WlanSvc		WLAN AutoConfig
wlidsvc		Microsoft Account Sign-in Assistant
wlpasvc		Local Profile Assistant Service
WManSvc		Windows Management Service
wmiApSrv		WMI Performance Adapter
WMPNetworkSvc		Windows Media Player Network Sharing Service
workfolderssvc		Work Folders
WpcMonSvc		Parental Controls
WPDBusEnum		Portable Device Enumerator Service
WpnService	started	Windows Push Notifications System Service
wscsvc	started	Security Center
WSearch	started	Windows Search
wuauserv		Windows Update
WwanSvc		WWAN AutoConfig
XblAuthManager		Xbox Live Auth Manager
XblGameSave		Xbox Live Game Save
XboxGipSvc		Xbox Accessory Management Service
XboxNetApiSvc		Xbox Live Networking Service
MozillaMaintenance		Mozilla Maintenance Service
AarSvc_5bb811		Agent Activation Runtime_5bb811
BcastDVRUserService_5bb811		GameDVR and Broadcast User Service_5bb811
BluetoothUserService_5bb811		Bluetooth User Support Service_5bb811
CaptureService_5bb811		CaptureService_5bb811
cbdhsvc_5bb811	started	Clipboard User Service_5bb811
CDPUserSvc_5bb811	started	Connected Devices Platform User Service_5bb811
ConsentUxUserSvc_5bb811		ConsentUX_5bb811
CredentialEnrollmentManagerUserSvc_5bb811		CredentialEnrollmentManagerUserSvc_5bb811
DeviceAssociationBrokerSvc_5bb811		DeviceAssociationBroker_5bb811
DevicePickerUserSvc_5bb811		DevicePicker_5bb811
DevicesFlowUserSvc_5bb811		DevicesFlow_5bb811
MessagingService_5bb811		MessagingService_5bb811

OneSyncSvc_5bb811	started	Sync Host_5bb811
PimIndexMaintenanceSvc_5bb811		Contact Data_5bb811
PrintWorkflowUserSvc_5bb811		PrintWorkflow_5bb811
UdkUserSvc_5bb811		Udk User Service_5bb811
UnistoreSvc_5bb811		User Data Storage_5bb811
UserDataSvc_5bb811		User Data Access_5bb811
WpnUserService_5bb811	started	Windows Push Notifications User Service_5bb811

 1 Windows Drivers List

QID:	90066
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/31/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following Windows drivers were detected.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Status	Description
1394ohci		1394 OHCI Compliant Host Controller
3ware		3ware
ACPI	started	Microsoft ACPI Driver
AcpiDev		ACPI Devices driver
acpiex	started	Microsoft ACPIEx Driver
acpipagr		ACPI Processor Aggregator Driver
AcpiPmi		ACPI Power Meter Driver
acpitime		ACPI Wake Alarm Driver
Acx01000		Acx01000
ADP80XX		ADP80XX
AFD	started	Ancillary Function Driver for Winsock
afunix	started	afunix
ahcache	started	Application Compatibility Cache
amdgpio2		AMD GPIO Client Driver
amdi2c		AMD I2C Controller Service
AmdK8		AMD K8 Processor Driver
AmdPPM		AMD Processor Driver
amdsata		amdsata
amdsbs		amdsbs
amdxata		amdxata

AppID		AppID Driver
applockerfltr		Smartlocker Filter Driver
AppvStrm		AppvStrm
AppvVemgr		AppvVemgr
AppvVfs		AppvVfs
arcsas		Adaptec SAS/SATA-II RAID Storport's Miniport Driver
AsyncMac		RAS Asynchronous Media Driver
atapi		IDE Channel
b06bdrv		QLogic Network Adapter VBD
bam	started	Background Activity Moderator Driver
BasicDisplay	started	BasicDisplay
BasicRender	started	BasicRender
bcmfn2		bcmfn2 Service
Beep	started	Beep
bindflt	started	Windows Bind Filter Driver
bowser	started	Browser
BthA2dp		Microsoft Bluetooth A2dp driver
BthEnum		Bluetooth Enumerator Service
BthHFEnum		Microsoft Bluetooth Hands-Free Profile driver
BthLEEnum		Bluetooth Low Energy Driver
BthMini		Bluetooth Radio Driver
BTHMODEM		Bluetooth Modem Communications Driver
BTHPORT		Bluetooth Port Driver
BTHUSB		Bluetooth Radio USB Driver
bttflt		Microsoft Hyper-V VHDPMEM BTT Filter
buttonconverter		Service for Portable Device Control devices
CAD	started	Charge Arbitration Driver
cdfs	started	CD/DVD File System Reader
cdrom	started	CD-ROM Driver
cht4iscsi		cht4iscsi
cht4vbd		Chelsio Virtual Bus Driver
CimFS	started	CimFS
circlass		Consumer IR Devices
CldFlt	started	Windows Cloud Files Filter Driver
CLFS	started	Common Log (CLFS)
CmBatt	started	Microsoft ACPI Control Method Battery Driver
CNG	started	CNG
cnghwassist		CNG Hardware Assist algorithm provider
CompositeBus	started	Composite Bus Enumerator Driver
condrv	started	Console Driver
CSC	started	Offline Files Driver
dam		Desktop Activity Moderator Driver
Dfsc	started	DFS Namespace Client Driver
disk	started	Disk Driver
dmvsc		dmvsc
drmkaud		Microsoft Trusted Audio Drivers
DXGKrnl	started	LDDM Graphics Subsystem
E1G60	started	Intel(R) PRO/1000 NDIS 6 Adapter Driver
ebdrv		QLogic 10 Gigabit Ethernet Adapter VBD
EhStorClass	started	Enhanced Storage Filter Driver
EhStorTcgDrv		Microsoft driver for storage devices supporting IEEE 1667 and TCG protocols
ErrDev		Microsoft Hardware Error Device Driver
exfat		exFAT File System Driver
fastfat		FAT12/16/32 File System Driver
fdc		Floppy Disk Controller Driver

FileCrypt	started	FileCrypt
FileInfo	started	File Information FS MiniFilter
Filetrace		Filetrace
flpydisk		Floppy Disk Driver
FltMgr	started	FltMgr
FsDepends		File System Dependency Minifilter
fvevol	started	BitLocker Drive Encryption Filter Driver
gencounter		Microsoft Hyper-V Generation Counter
genericusbfn		Generic USB Function Class
GPIOClx0101		Microsoft GPIO Class Extension Driver
GpuEnergyDrv	started	GPU Energy Driver
HdAudAddService	started	Microsoft 1.1 UAA Function Driver for High Definition Audio Service
HDAudBus	started	Microsoft UAA Bus Driver for High Definition Audio
HidBatt		HID UPS Battery Driver
HidBth		Microsoft Bluetooth HID Miniport
hidi2c		Microsoft I2C HID Miniport Driver
hidinterrupt		Common Driver for HID Buttons implemented with interrupts
HidIr		Microsoft Infrared HID Driver
hidspi		Microsoft SPI HID Miniport Driver
HidSpiCx		HidSpi KMDF Class Extension
HidUsb	started	Microsoft HID Class Driver
HpSAMD		HpSAMD
HTTP	started	HTTP Service
hvcrash		hvcrash
hvservice		Hypervisor/Virtual Machine Support Driver
HwNClx0101		Microsoft Hardware Notifications Class Extension Driver
hwpolicy		Hardware Policy Driver
hyperkbd		hyperkbd
HyperVideo		HyperVideo
i8042prt	started	i8042 Keyboard and PS/2 Mouse Port Driver
iagpio		Intel Serial IO GPIO Controller Driver
iai2c		Intel(R) Serial IO I2C Host Controller
iaLPSS2i_GPIO2		Intel(R) Serial IO GPIO Driver v2
iaLPSS2i_GPIO2_BXT_P		Intel(R) Serial IO GPIO Driver v2
iaLPSS2i_GPIO2_CNL		Intel(R) Serial IO GPIO Driver v2
iaLPSS2i_GPIO2_GLK		Intel(R) Serial IO GPIO Driver v2
iaLPSS2i_I2C		Intel(R) Serial IO I2C Driver v2
iaLPSS2i_I2C_BXT_P		Intel(R) Serial IO I2C Driver v2
iaLPSS2i_I2C_CNL		Intel(R) Serial IO I2C Driver v2
iaLPSS2i_I2C_GLK		Intel(R) Serial IO I2C Driver v2
iaLPSSi_GPIO		Intel(R) Serial IO GPIO Controller Driver
iaLPSSi_I2C		Intel(R) Serial IO I2C Controller Driver
iaStorAVC		Intel Chipset SATA RAID Controller
iaStorV		Intel RAID Controller Windows 7
ibbus		Mellanox InfiniBand Bus/AL (Filter Driver)
IndirectKmd		Indirect Displays Kernel-Mode Driver
intelide		intelide
intelpep	started	Intel(R) Power Engine Plug-in Driver
intelpmax		Intel(R) Dynamic Device Peak Power Manager Driver
intelppm	started	Intel Processor Driver
iorate	started	Disk I/O Rate Filter Driver
IpFilterDriver		IP Traffic Filter Driver
IPMIDRV		IPMIDRV
IPNAT		IP Network Address Translator
IPT		IPT

isapnp		isapnp
iScsiPrt		iScsiPort Driver
ItSas35i		ItSas35i
kbdclass	started	Keyboard Class Driver
kbdhid		Keyboard HID Driver
kbldfltr		kbldfltr
kdnic	started	Microsoft Kernel Debug Network Miniport (NDIS 6.20)
KSecDD	started	KSecDD
KSecPkg	started	KSecPkg
ksthunk	started	Kernel Streaming Thunks
lltdio	started	Link-Layer Topology Discovery Mapper I/O Driver
LSI_SAS		LSI_SAS
LSI_SAS2i		LSI_SAS2i
LSI_SAS3i		LSI_SAS3i
LSI_SSS		LSI_SSS
luafv	started	UAC File Virtualization
mausbhost		MA-USB Host Controller Driver
mausbip		MA-USB IP Filter Driver
MbbCx		MBB Network Adapter Class Extension
megasas		megasas
megasas2i		megasas2i
megasas35i		megasas35i
megasr		megasr
Microsoft_Bluetooth_AvrcpTransport		Microsoft Bluetooth Avrcp Transport Driver
mlx4_bus		Mellanox ConnectX Bus Enumerator
MMCSS	started	Multimedia Class Scheduler
Modem		Modem
monitor	started	Microsoft Monitor Class Function Driver Service
mouclass	started	Mouse Class Driver
mouhid	started	Mouse HID Driver
mountmgr	started	Mount Point Manager
mpsdrv	started	Windows Defender Firewall Authorization Driver
MRxDAV		WebDav Client Redirector Driver
mrxsmb	started	SMB MiniRedirector Wrapper and Engine
mrxsmb20	started	SMB 2.0 MiniRedirector
MsBridge		Microsoft MAC Bridge
Msfs	started	Msfs
msgpiowin32		Common Driver for Buttons, DockMode and Laptop/Slate Indicator
mshidkmdf		Pass-through HID to KMDF Filter Driver
mshidumdf		Pass-through HID to UMDF Driver
msisadrv	started	msisadrv
MSKSSRV		Microsoft Streaming Service Proxy
MsLldp	started	Microsoft Link-Layer Discovery Protocol
MSPCLOCK		Microsoft Streaming Clock Proxy
MSPQM		Microsoft Streaming Quality Manager Proxy
MsQuic	started	MsQuic
MsRPC		MsRPC
MsSecCore	started	Microsoft Security Core Boot Driver
MsSecFlt		Microsoft Security Events Component Minifilter
MsSecWfp		Microsoft Security WFP Callout Driver
mssmbios	started	Microsoft System Management BIOS Driver
MSTEE		Microsoft Streaming Tee/Sink-to-Sink Converter
MTConfig		Microsoft Input Configuration Driver
Mup	started	Mup
mvumis		mvumis

NativeWifiP		NativeWiFi Filter
ndfltr		NetworkDirect Service
NDIS	started	NDIS System Driver
NdisCap	started	Microsoft NDIS Capture
NdisImPlatform		Microsoft Network Adapter Multiplexor Protocol
NdisTapi		Remote Access NDIS TAPI Driver
Ndisuio		NDIS Usermode I/O Protocol
NdisVirtualBus	started	Microsoft Virtual Network Adapter Enumerator
NdisWan		Remote Access NDIS WAN Driver
ndiswanlegacy		Remote Access LEGACY NDIS WAN Driver
NDKPing		NDKPing Driver
ndproxy		NDIS Proxy Driver
Ndu	started	Windows Network Data Usage Monitoring Driver
NetAdapterCx		Network Adapter Wdf Class Extension Library
NetBIOS	started	NetBIOS Interface
NetBT	started	NetBT
netvsc		netvsc
Npfs	started	Npfs
npsvctrig	started	Named pipe service trigger provider
nsiproxy	started	NSI Proxy Service Driver
Ntfs	started	Ntfs
Null	started	Null
nvdimm		Microsoft NVDIMM device driver
nvraid		nvraid
nvstor		nvstor
Parport		Parallel port driver
partmgr	started	Partition driver
pci	started	PCI Bus Driver
pciide		pciide
pcmcia		pcmcia
pcw	started	Performance Counters for Windows Driver
pdc	started	pdc
PEAUTH	started	PEAUTH
percsas2i		percsas2i
percsas3i		percsas3i
PktMon		Packet Monitor Driver
pmem		Microsoft persistent memory disk driver
PNPMEM		Microsoft Memory Module Driver
portcfg		portcfg
PptpMiniport		WAN Miniport (PPTP)
Processor		Processor Driver
Psched	started	QoS Packet Scheduler
QWAVEdrv		QWAVE driver
Ramdisk		Windows RAM Disk Driver
RasAcd		Remote Access Auto Connection Driver
RasAgileVpn		WAN Miniport (IKEv2)
Rasl2tp		WAN Miniport (L2TP)
RasPppoe		Remote Access PPPOE Driver
RasSstp		WAN Miniport (SSTP)
rdbss	started	Redirected Buffering Sub System
rdpbus	started	Remote Desktop Device Redirector Bus Driver
RDPDR		Remote Desktop Device Redirector Driver
RdpVideoMiniport		Remote Desktop Video Miniport Driver
rdyboost	started	ReadyBoost
ReFS		ReFS

ReFSv1		ReFSv1
RFCOMM		Bluetooth Device (RFCOMM Protocol TDI)
rhproxy		Resource Hub proxy driver
rspndr	started	Link-Layer Topology Discovery Responder
s3cap		s3cap
sbp2port		SBP-2 Transport/Protocol Bus Driver
scfilter		Smart card PnP Class Filter Driver
scmbus		Microsoft Storage Class Memory Bus Driver
sdbus		sdbus
SDFRd		SDF Reflector
sdstor		SD Storage Port Driver
SerCx		Serial UART Support Library
SerCx2		Serial UART Support Library
Serenum		Serenum Filter Driver
Serial		Serial port driver
sermouse		Serial Mouse Driver
sfloppy		High-Capacity Floppy Disk Drive
SgrmAgent	started	System Guard Runtime Monitor Agent
SiSRaid2		SiSRaid2
SiSRaid4		SiSRaid4
SmartSAMD		SmartSAMD
smbdirect		smbdirect
spaceparser		Space Parser
spaceport	started	Storage Spaces Driver
SpatialGraphFilter		Holographic Spatial Graph Filter
SpbCx		Simple Peripheral Bus Support Library
srv2	started	Server SMB 2.xxx Driver
srvnet	started	srvnet
stexstor		stexstor
storahci	started	Microsoft Standard SATA AHCI Driver
storflt		Microsoft Hyper-V Storage Accelerator
stornvme		Microsoft Standard NVM Express Driver
storqosflt	started	Storage QoS Filter Driver
storufs		Microsoft Universal Flash Storage (UFS) Driver
storvsc		storvsc
swenum	started	Software Bus Driver
Synth3dVsc		Synth3dVsc
Tcpip	started	TCP/IP Protocol Driver
Tcpip6		@todo.dll, -100;Microsoft IPv6 Protocol Driver
tcpipreg	started	TCP/IP Registry Compatibility
tdx	started	NetIO Legacy TDI Support Driver
Telemetry	started	Intel(R) Telemetry Service
terminpt		Microsoft Remote Desktop Input Driver
TPM		TPM
TsUsbFlt		Remote Desktop USB Hub Class Filter Driver
TsUsbGD		Remote Desktop Generic USB Device
tsusbhub		Remote Desktop USB Hub
tunnel		Microsoft Tunnel Miniport Adapter Driver
UASPStor		USB Attached SCSI (UAS) Driver
UcmCx0101		USB Connector Manager KMDF Class Extension
UcmTcpciCx0101		UCM-TCPCI KMDF Class Extension
UcmUcsiAcpiClient		UCM-UCSI ACPI Client
UcmUcsiCx0101		UCM-UCSI KMDF Class Extension
UCPD		UCPD
Ucx01000	started	USB Host Support Library

UdeCx		USB Device Emulation Support Library
udfs		udfs
UEFI		Microsoft UEFI Driver
UevAgentDriver		UevAgentDriver
Ufx01000		USB Function Class Extension
UfxChipidea		USB Chipidea Controller
ufxsynopsys		USB Synopsys Controller
umbus	started	UMBus Enumerator Driver
UmPass	started	Microsoft UMPass Driver
UrsChipidea		Chipidea USB Role-Switch Driver
UrsCx01000		USB Role-Switch Support Library
UrsSynopsys		Synopsys USB Role-Switch Driver
usbaudio		USB Audio Driver (WDM)
usbaudio2		USB Audio 2.0 Service
usbccgp		Microsoft USB Generic Parent Driver
usbcir		eHome Infrared Receiver (USBCIR)
usbehci		Microsoft USB 2.0 Enhanced Host Controller Miniport Driver
usbhub		Microsoft USB Standard Hub Driver
USBHUB3	started	SuperSpeed Hub
usbohci		Microsoft USB Open Host Controller Miniport Driver
usbprint		Microsoft USB PRINTER Class
usbser		Microsoft USB Serial Driver
USBSTOR		USB Mass Storage Driver
usbuhci		Microsoft USB Universal Host Controller Miniport Driver
USBXHCI	started	USB xHCI Compliant Host Controller
VBoxGuest	started	VirtualBox Guest Driver
VBoxMouse	started	VirtualBox Guest Mouse Service
VBoxSF	started	VirtualBox Shared Folders
VBoxWddm	started	VBoxWddm
vdrvroot	started	Microsoft Virtual Drive Enumerator
VerifierExt		Driver Verifier Extension
vhdmp		vhdmp
vhf		Virtual HID Framework (VHF) Driver
Vid	started	Vid
VirtualRender		VirtualRender
vmbus		Virtual Machine Bus
VMBusHID		VMBusHID
vmgid		Microsoft Hyper-V Guest Infrastructure Driver
volmgr	started	Volume Manager Driver
volmgrx	started	Dynamic Volume Manager
volsnap	started	Volume Shadow Copy driver
volume	started	Volume driver
vpci		Microsoft Hyper-V Virtual PCI Bus
vsmraid		vsmraid
VSTXRAID		VIA StorX Storage RAID Controller Windows Driver
vwifibus		Virtual Wireless Bus Driver
vwififlt	started	Virtual WiFi Filter Driver
WacomPen		Wacom Serial Pen HID Driver
wanarp		Remote Access IP ARP Driver
wanarpv6		Remote Access IPv6 ARP Driver
wcifs	started	Windows Container Isolation
wcnfs		Windows Container Name Virtualization
WdBoot		Microsoft Defender Antivirus Boot Driver
Wdf01000	started	Kernel Mode Driver Frameworks service
WdFilter	started	Microsoft Defender Antivirus Mini-Filter Driver

wdiwifi		WDI Driver Framework
WdmCompanionFilter		WdmCompanionFilter
WdNisDrv	started	Microsoft Defender Antivirus Network Inspection System Driver
WFPLWFS	started	Microsoft Windows Filtering Platform
WIMMount		WIMMount
WindowsTrustedRT	started	Windows Trusted Execution Environment Class Extension
WindowsTrustedRTProxy	started	Microsoft Windows Trusted Runtime Secure Service
WinMad		WinMad Service
WinNat		Windows NAT Driver
WINUSB		WinUsb Driver
WinVerbs		WinVerbs Service
WmiAcpi		Microsoft Windows Management Interface for ACPI
Wof	started	Windows Overlay File System Filter Driver
WpdUpFltr		WPD Upper Class Filter Driver
ws2ifsl		Winsock IFS Driver
WudfPf		User Mode Driver Frameworks Platform Driver
WUDFRd		Windows Driver Foundation - User-mode Driver Framework Reflector
xboxgip		Xbox Game Input Protocol Driver
xinputhid		XINPUT HID Filter Driver

1 Programs Launched At Startup Through The Registry

QID:	90074
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Windows launches a number of programs automatically at system startup. These programs are frequently used by legitimately installed software. It's possible for malware to be opened automatically as well.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SecurityHealth = %windir%\system32\SecurityHealthSystray.exe
VBoxTray = %SystemRoot%\system32\VBoxTray.exe

1 Windows Product Type

QID:	90107
Category:	Windows
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/07/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The results below identify which type of Windows product is installed:
- If ProductType is "Winnt", the host is running Windows

Workstation.
- If ProductType is "Servernt", the host is running Windows Server.
- If ProductType is "Lanmannt", the

host is running Windows Advanced Server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows NT\CurrentVersion		
BuildBranch	=	vb_release
BuildLabEx	=	19041.1.amd64fre.vb_release.191206-1406
CurrentBuild	=	19045
CurrentBuildNumber	=	19045
CurrentVersion	=	6.3
EditionID	=	Professional
InstallationType	=	Client
ProductName	=	Windows 10 Pro
ReleaseId	=	2009
UBR	=	3803
DisplayVersion	=	22H2
HKLM\SYSTEM\currentControlSet\Control\ProductOptions		
ProductType	=	WinNT
ProductSuite	=	{"Terminal Server"}

1 Windows Internet Explorer Version

QID:	90295
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/27/2013

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows Internet Explorer version is shown.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Windows Internet Explorer 11.0.19041.3636

 1 Access to File Share is Enabled

QID:	90331
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/18/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The purpose of this QID is to indicate that access to the file share on the target host has been enabled. While the overwhelming majority of checks for Microsoft Windows and other Microsoft products rely simply on registry access via the winreg named pipe, checks for several third party products rely on file version checks which require file share access. This QID is posted if ntoskrnl.exe, which is found on all Windows systems, is detected on the target host.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management

Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

Type: SOX
Section: N/A
Description: User Access Management Granting resource access, user ID and password requirements, individual accountability, limited utilization of native administrative IDs, non-employee user ID expiration, reporting employee and contractor status changes. Operating System Access Control Password enforcement, logon information, password display and printing, required password changes, vendor default passwords, security changes after system compromise, systems software utility usage, automatic log off. Password Management Procedures exist that ensure the confidentiality and protection of passwords through secure password creation and distribution mechanisms, the enforcement and adherence to acceptable password standards, and the regular changing of passwords.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%SystemRoot%\system32\ntoskrnl.exe found

1 Windows File Access Denied

QID:	90399
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/02/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote access to the following files has been denied. Access to the share was successful, but remote access to the files in the Result section has been denied.

IMPACT:

Vulnerabilities that require file access may not have been detected during the scan.

SOLUTION:

See the permissions assigned to the provided user authentication credentials, and ensure that the credentials provide read access to the boot share. On Windows XP Professional use Classic for local network logins (default is Guest only, which prohibits file access). Using the Group Policy editor, this may be set at Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

File path	Error code

C:\DumpStack.log.tmp	C0000043
C:\pagefile.sys	C0000043
C:\swapfile.sys	C0000043
C:\Windows\CSC	C0000022

1 Microsoft Windows Last Reboot Date and Time

QID:	90924
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/02/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

System last reboot date and time.Note: WMI services is required for the execution of this query.

IMPACT:

N/A

SOLUTION:

N/A

Workaround:N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Last Reboot Date and Time(yyyy/mm/dd hh:mm:ss): 2024/09/23 11:10:58

1 Microsoft Windows User Last Logon Time

QID:	90925
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/25/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows User Last Logon Time.Note: WMI services is required for the execution of this query.

IMPACT:

N/A

SOLUTION:

N/A

Workaround:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

'C:\\Users\\User'	2024/09/23 16:08:01
'C:\\Windows\\ServiceProfiles\\NetworkService'	2024/09/23 16:08:01
'C:\\Windows\\ServiceProfiles\\LocalService'	2024/09/23 16:08:01
'C:\\Windows\\system32\\config\\systemprofile'	2024/09/23 16:08:01

1 Operating System's Install Date and Time

QID:	91074
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID detects the "Install Date" of the targeted Microsoft Windows installation.
It does so by utilizing either of the following methods:
1. Querying the Windows Management Instrumentation (WMI) specification for the InstallDate function.
2. Queries a certain Windows Registry location to fetch this value.

NOTE: For the WMI query to work, the WMI service (winmgmt) should be enabled.

Unlike the availability of "Operating System InstallDate" from Windows Registry Entry.
For Linux and MacOS, there is no Direct Way to Collect "Operating System InstallDate Time".
Attempt has been made to provide the Most Appropriate Date and time of OS install Date.
1. Based on TIMESTAMPS of /boot, /, BaseSystem RPMS and Files in /etc/

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Microsoft Windows install date retrieved from the registry: Monday, September 23, 2024 14:58:49 GMT

1 List of Microsoft Patches Installed on System

QID:	91328
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/27/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft patches listed using wmi or windows registry keys.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HotfixID
'KB5031988'
'KB5015684'
'KB5033372'
'KB5014032'
'KB5032907'

1 Java Enabled in the Internet Zone

QID:	100141
Category:	Internet Explorer

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/15/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The target has Java enabled in the Internet Zone (Zone 3).

The Java Permissions setting (1C00) has the following five possible values (binary):

```
Value    Setting
-----------------------
00 00 00 00 Disable Java
00 00 01 00 High safety
00 00 02 00 Medium safety
00 00 03 00 Low safety
00 00 80 00 Custom
```

This QID will flag if Java is enabled (has any value apart from 0)

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Java enabled in Internet Zone in HKLM hive
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 1C00 = 65536

 1 Microsoft Internet Explorer 11 Detected

QID:	100274
Category:	Internet Explorer
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/13/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft Internet Explorer 11 is installed on the machine.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Internet Explorer Version = 9.11.19041.0

1 Windows Registry Access Level

QID:	105025
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner can access these registry keys, which are important for performing patch verification.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths
Machine = System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog

1 Microsoft Windows System Hardware Enumeration, CPU

QID:	105054
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/27/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows system CPU information for this host is enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0

Identifier	=	Intel64 Family 6 Model 142 Stepping 10
ProcessorNameString	=	Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz
VendorIdentifier	=	GenuineIntel
~MHz	=	1896

1 Microsoft Windows System Hardware Enumeration, Display Devices

QID:	105056
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/22/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Information about the display devices on this system is provided in the Result section. With this information, you can determine the manufacturer of the device and then contact the manufacturer for device updates. You can also verify the display resolution, which helps troubleshoot display problems.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_80EE&DEV_BEEF&SUBSYS_040515AD&REV_00\3&267a616a&0&10\Control	{4d36e968-e325-11ce-bfc1-08002be10318}\0000
Dev:	@oem3.inf, %vboxwddm.svcdesc%;VirtualBox Graphics Adapter (WDDM)
Manufacturer:	@oem3.inf, %oracle%;Oracle Corporation
Service:	VBoxWddm
Driver Instance:	{4d36e968-e325-11ce-bfc1-08002be10318}\0000
Driver Description:	VirtualBox Graphics Adapter (WDDM)
Driver_Date:	9-6-2024
Driver_Version:	7.1.0.14728

1 Microsoft Windows System Hardware Enumeration, Input Devices

QID:	105058
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Keyboard and pointing device details of this Windows system are enumerated. Information about your keyboard, pointing device ("mouse"), and other input devices is provided.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Enum\ACPI\PNP0F03\4&1d401fb5&0\Control	{4d36e96f-e325-11ce-bfc1-08002be10318}\0000			
Dev:	@msmouse.inf, %*pnp0f03.devicedesc%;Microsoft PS/2 Mouse			
Manufacturer:	@msmouse.inf, %msmfg%;Microsoft			
Service:	i8042prt			
Driver Instance:	{4d36e96f-e325-11ce-bfc1-08002be10318}\0000			
Driver Description:	Microsoft PS/2 Mouse			
Driver_Date:	6-21-2006			
Driver_Version:	10.0.19041.1			
HKLM\SYSTEM\CurrentControlSet\Enum\ACPI\PNP0303\4&1d401fb5&0\Control	{4d36e96b-e325-11ce-bfc1-08002be10318}\0000			
Dev:	@keyboard.inf, %*pnp0303.devicedesc%;Standard	PS/2	Keyboard	
Manufacturer:	@keyboard.inf, %std-keyboards%;(Standard	keyboards)		
Service:	i8042prt			
Driver	Instance:	{4d36e96b-e325-11ce-bfc1-08002be10318}\0000		
Driver	Description:	Standard	PS/2	Keyboard
Driver Date:	6-21-2006			
Driver Version:	10.0.19041.1			

1 Microsoft Windows System Hardware Enumeration, Networking Components

QID:	105059
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The network components are enumerated and information presented in three subcategories: Adapter, Protocol, and WinSock. These subcategories display information about the network adapters, protocols, and WinSock settings on the host system. Support engineers and network administrators can use this information to verify network configurations.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_8086&DEV_100E&SUBSYS_001E8086&REV_02\3&267a616a&0&18\Control	{4d36e972-e325-11ce-bfc1-08002be10318}\0001
Dev:	@nete1g3e.inf, %e100e.devicedesc%;Intel(R) PRO/1000 MT Desktop Adapter
Manufacturer:	@nete1g3e.inf, %intel%;Intel
Service:	E1G60
Driver Instance:	{4d36e972-e325-11ce-bfc1-08002be10318}\0001
Driver Description:	Intel(R) PRO/1000 MT Desktop Adapter
Driver_Date:	3-23-2010
Driver_Version:	8.4.13.0

1 Microsoft Windows Audit Settings Enumerated From LSA

QID:	105063
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/07/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The account audit configuration is enumerated. The audit settings are:

Audit System Events
Audit Logon Events
Audit Object Access
Audit Privilege Use
Audit Process Tracking
Audit Policy Change
Audit Account Management
Audit Directory Service Access
Audit Account Logon

You should specify an administrator privileged user in the "Windows Authentication Record" preferences of Qualys for this detection to be successful.

IMPACT:

N/A

SOLUTION:

It is advised to log at least the logon events as a best practice.

Use the MMC snapin "Administrative Tools" - "Local Security Policy" to change the settings. These options are listed under "Local Policy" - "Audit Policy".

COMPLIANCE:

Type: CobIT
Section: N/A
Description: The IT Management Official (or Technology Architecture Manager) ensures audit trail/system upgrade histories are stored in a secure location with update/delete access granted on a strict business need only basis to technology support personnel.

Type: HIPAA

Section: 164.308(a)(5)(ii)(C)
Description: Log-In Monitoring
Procedures for monitoring log-in attempts and reporting discrepancies.

Type: SOX
Section: N/A
Description: Event capture/violation logging is enabled at the operating system to record the following:
- All significant security relevant events including, but not limited to, invalid password guessing attempts, failed attempts to use privileges or resources that are not authorized
- All user ID creation, deletion, and privilege change activity performed by system administrators and others with privileged user IDs

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Audit system events	No Auditing
Audit logon events	No Auditing
Audit object access	No Auditing
Audit privilege use	No Auditing
Audit process tracking	No Auditing
Audit policy change	No Auditing
Audit account management	No Auditing
Audit directory service access	No Auditing
Audit account logon events	No Auditing

1 File Access Permissions for Regedt32.exe

QID:	105141
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/28/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Registry Editors allow administrators and applications to tweak the system. Malicious users with unauthorized access could compromise the system or gather sensitive information about it from the registry. Access to registry editors should be limited to only the authorized administrative users. The permissions for the target's regedit32.exe registry editor binaries are listed in the Result section below.

IMPACT:

N/A

SOLUTION:

Verify that only legitimate administrative, authorized users have access to the registry editors.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\system32\regedt32.exe NT SERVICE\TrustedInstaller 2271478464 access_allowed standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes
%windir%\system32\regedt32.exe Administrators 544 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\system32\regedt32.exe SYSTEM 18 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\system32\regedt32.exe Users 545 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\system32\regedt32.exe APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES 1 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\system32\regedt32.exe APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES 2 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes

1 File Access Permissions for Regedit.exe

QID:	105154
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Registry Editors allow administrators and applications to tweak the system. Malicious users with unauthorized access could compromise the system or gather sensitive information about it from the registry. Access to registry editors should be limited to only the authorized administrative users. The permissions for the host's registry editor binary "regedit.exe" are listed in the Result section below.

IMPACT:

N/A

SOLUTION:

Verify that only legitimate administrative, authorized users have access to the registry editors.

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\regedit.exe NT SERVICE\TrustedInstaller 2271478464 access_allowed standard_write_dac synchronize append_data standard_read execute standard_write_owner write_data write_extended_attributes read_data read_attributes write_attributes delete_child standard_delete read_extended_attributes

%windir%\regedit.exe Administrators 544 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\regedit.exe SYSTEM 18 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\regedit.exe Users 545 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\regedit.exe APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES 1 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes
%windir%\regedit.exe APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES 2 access_allowed synchronize standard_read execute read_data read_attributes read_extended_attributes

1 Microsoft Windows System EventLog Policy Parameters

QID:	105165
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/18/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This reports the EventLog parameters for the System database that are of interest to compliance audits. These configurations exist under this registry subkey:

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System

RestrictGuestAccess - Setting this to 1 prevents guests and anonymous user accounts from having read access to the System EventLog.

MaxSize - This value specifies tha maximum size limit for the System EventLog database.

Retention - This value specifies the overwrite behavior for the System EventLog. 0 means overwrite as needed. 0xffffffff means do not overwrite events, and other values specify number of days that eventlog entries are preserved before overwriting.

IMPACT:

N/A

SOLUTION:

Configure the System EventLog by changing the registry values to appropriate values, or use the EventViewer GUI to change the parameters.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System

MaxSize	=	20971520
Retention	=	0
RestrictGuestAccess	=	1

1 Microsoft Windows Application EventLog Policy Parameters

QID:	105166
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	04/18/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This reports the EventLog parameters for the System database that are of interest to compliance audits. These configurations exist under this registry subkey:

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application

RestrictGuestAccess - Setting this to 1 prevents guests and anonymous user accounts from having read access to the Application EventLog database.

MaxSize - This value specifies tha maximum size limit for the Application EventLog database.

Retention - This value specifies the overwrite behavior for the Application EventLog. 0 means overwrite as needed. 0xffffffff means do not overwrite events, and other values specify the number of days of eventlog entries that are preserved before overwriting.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application		
MaxSize	=	20971520
Retention	=	0
RestrictGuestAccess	=	1

1 Microsoft Windows Security EventLog Policy Parameters

QID:	105167
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/07/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This reports the EventLog parameters for the Security database that are of interest to compliance audits. These configurations exist under this registry subkey:

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

RestrictGuestAccess - Setting this to 1 prevents guests and anonymous user accounts from having read access to the Security EventLog.

MaxSize - This value specifies tha maximum size limit for the Security EventLog database.

Retention - This value specifies the overwrite behavior for the Security EventLog. 0 means overwrite as needed. 0xffffffff means do not overwrite events, and other values specify the number of days of eventlog entries that are preserved before overwriting.

IMPACT:

N/A

SOLUTION:

Configure the Security Eventlog by changing the registry values to appropriate values or use the EventViewer GUI to change the parameters.

COMPLIANCE:

Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security		
MaxSize	=	20971520
Retention	=	0
RestrictGuestAccess	=	1

1 Message For Users Attempting To Logon To Windows System

QID:	105179
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows has a log-on notice setting that allows administrators to display a legal notice prior to users logging in. This check tests to see if the legal log-on notice is set at the target and enumerates the current value.

IMPACT:

This notice is used to ensure that sensitive systems are only accessed by authorized personnel.

SOLUTION:

The legal text can be added through the local security policy GUI or through the following registry values under the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

LegalNoticeCaption (REG_SZ) and LegalNoticeText (REG_SZ)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon
LegalNoticeCaption =
LegalNoticeText =
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
legalnoticecaption =
legalnoticetext =

1 Windows Builtin User Group Membership Audit - Backup Operators

QID:	105239
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The members of the Backup Operators Group are enumerated. It is essential to make sure unauthorized users are not part of this builtin group.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Backup Operators No members in this group

1 Windows Builtin User Group Membership Audit - Replicator

QID:	105240

Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

User accounts that are members of the Replicator Group are enumerated from the target host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Replicator No members in this group

1 Windows Builtin User Group Membership Audit - Network Configuration Operators

QID:	105241
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The user accounts that are members of the Network Configuration Operators group are enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Network Configuration Operators No members in this group

1 IPSEC Policy Agent Service Status Detected

QID:	105256
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/28/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The status of IPSEC Policy Agent Service at the target Windows machine is enumerated.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

PolicyAgent = RUNNING

1 Internet Explorer Search Companion Setting

QID:	105291
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/14/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Search Companion settings for users are enumerated from the target Microsoft Windows machine. Search Companion is a feature integrated into Internet Explorer that allows Internet searches for files using a web service hosted by Microsoft.

IMPACT:

N/A

SOLUTION:

Search Companion can be disabled using the Internet Explorer GUI.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KEY:	Software\Microsoft\Internet Explorer\Main	Use Search Asst
Local_System	Last Change:	value_missing_Q
Local_Service	Last Change:	value_missing_Q
Network_Service	Last Change:	value_missing_Q
DESKTOP-LN5HE01\User	Last Change:	value_missing_Q

 1 Microsoft Defender Installed

QID:	105310
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/10/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows Defender is installed on the target host. This Qid will detect the status of Windows Defender service, file version, real time protection on/off and signature last updated date.

IMPACT:

n/a

SOLUTION:

n/a

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WinDefend is RUNNING LocalSystem
Windows Defender 4.18.1909.6
From Local Registry Windows Defender ASSignatureApplied Value is: Tuesday, September 24, 2019 05:12:58 GMT
From Local Registry Windows Defender AVSignatureApplied Vaule is: Tuesday, September 24, 2019 05:12:58 GMT
HKLM\SOFTWARE\Microsoft\Windows Defender
ProductAppDataPath = C:\ProgramData\Microsoft\Windows Defender
ProductIcon = @%ProgramFiles%\Windows Defender\EppManifest.dll,-100
ProductLocalizedName = @%ProgramFiles%\Windows Defender\EppManifest.dll,-1000
RemediationExe = windowsdefender://
ProductType = 2
InstallTime = cafe30ebe10ddb01
InstallLocation = C:\Program Files\Windows Defender\
ManagedDefenderProductType = 0
OOBEInstallTime = 9be63b28ca0ddb01
ProductStatus = 0

HKLM\SOFTWARE\Microsoft\Windows Defender\Features
TamperProtection = 0
MpPlatformKillbitsFromEngine = 0000000000004000

HKLM\SOFTWARE\Microsoft\Windows Defender\MpEngine
MpCampGradualRelease = 1
MpCampRing = 2
MpEngineRing = 2

HKLM\SOFTWARE\Microsoft\Windows Defender\Quarantine
PurgeItemsAfterDelay = 90

HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
DpaDisabled = 0

HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting
LastRtpAndScanConfigsCollectedInHeartbeatTime = 1ee7a312e20ddb01
SigUpdateTimestampsSinceLastHB =
LastRebootTime = 73298ac6ca0ddb01

HKLM\SOFTWARE\Microsoft\Windows Defender\Scan
4BCF5C7C-0000-0000-0000-300300000000 = C:\ProgramData\Microsoft\Windows
Defender\Scans\History\CacheManager\4BCF5C7C-0000-0000-0000-300300000000-0.bin
SFCState = 128
DaysUntilAggressiveCatchupQuickScan = 30
AggressiveCatchupQuickScanReattemptElapsed = 23
CacheFile = C:\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\4BCF5C7C-0000-0000-0000-300300000000-0.bin
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Signature Updates
DisableDefaultSigs = 0
SignatureCategoryID = 8c3fcc84-7410-4a95-8b89-a166a0190486
EngineVersion = 1.1.16400.2
AVSignatureVersion = 1.303.25.0
AVSignatureBaseVersion = 1.303.0.0
AVSignatureApplied = 0029afba9672d501
ASSignatureVersion = 1.303.25.0
ASSignatureBaseVersion = 1.303.0.0
ASSignatureApplied = 0029afba9672d501
SignatureLocation = C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default
SignatureType = 0

HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet
SpyNetReporting = 2
SubmitSamplesConsent = 1
SpyNetReportingLocation =
SOAP:https://wdcp.microsoft.com/WdCpSrvc.asmx,SOAP:https://wdcpalt.microsoft.com/WdCpSrvc.asmx,REST:https://wdcp.microsoft.com/wdcp.svc/submit
Report,REST:https://wdcpalt.microsoft.com/wdcp.svc/submitReport,BOND:https://wdcp.microsoft.com/wdcp.svc/bond/submitreport,BOND:https://wdcpal
t.microsoft.com/wdcp.svc/bond/submitreport
SSLOptions = 3
MAPSconcurrency = 1
MAPSconcurrencyDss = 10
LastMAPSSuccessTime = 1f173243cd0ddb01
LastMAPSFailureTime = 2af3afb8cc0ddb01

Malware Protection Engine Version:
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Default\mpengine.dll Version is 1.1.16400.2

1 Microsoft System Center Configuration Manager Client (SCCM) Not Installed

QID:	105504
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/31/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The remote host does not have the Microsoft System Center Configuration Manger Client installed.

System Center Configuration Manager is a solution to assess, deploy, and update servers, clients, and devices-across physical, virtual, distributed, and mobile environments.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\smstsmgr is missing

1 Disk Usage Information

QID:	115046
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/23/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The result section shows the amount of free space left on currently mounted drives.

Added Support for Windows Platform.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CAPTION FREESPACE SIZE
C: 32135139328 53058154496
D: 0 58832896

1 Memory Information

QID:	115049
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/28/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The results section shows the total amount of free and used physical memory and swap space on the host system in bytes. It also shows buffers and cache consumed by the kernel.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TotalPhysicalMemory : 2147012608

1 Windows Forensics MRU Enumeration - Regedit.exe

QID:	125017
Category:	Forensics

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This test enumerates the last edited key by the regedit.exe utility.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Key:	Software\Microsoft\Windows\CurrentVersion\Applets\Regedit	Value:	Lastkey
User:	DESKTOP-LN5HE01\User	VAL:	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

1 Installed Software information enumerated from all users using HKU registry key

QID:	372899
Category:	Local
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/14/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID enumerates the installed software from registry key "HKU" for all users.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Display Name	Display Version	Install Date	Publisher	Language	Install Path	User	Sid
Microsoft OneDrive	21.220.1024.0005		Microsoft Corporation			DESKTOP-LN5HE01\User	S-1-5-21-4268673589-654920014-3518733957-1001

Appendix

Hosts Scanned (IP)

10.0.0.197

Target distribution across scanner appliances

Testing : 10.0.0.197

Windows authentication was successful for these hosts (1)

Instance os:
10.0.0.197

Options Profile

Test Scan

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco/Network SSH:	Disabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled

Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Cassandra:	Disabled
MarkLogic:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

Severity	Level	Description
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.