Qualys. Community Edition

# Scan Results

December 21, 2023

| Report Summary | |
|---|---|
| User Name: | Khadijah Watkins |
| Login Name: | crena6kw |
| Company: | log |
| User Role: | Manager |
| Address: | 44 freshmont st |
| State: | Hawaii |
| Zip: | 89142 |
| Country: | United States of America |
| Created: | 12/21/2023 at 14:09:54 (GMT) |
| Launch Date: | 12/21/2023 at 05:49:29 (GMT) |
| Active Hosts: | 1 |
| Total Hosts: | 1 |
| Type: | On demand |
| Status: | Finished |
| Reference: | scan/1703137770.35222 |
| Scanner Appliances: | kdee (Scanner 12.16.55-1, Vulnerability Signatures 2.5.940-4) |
| Authentication: | Windows authentication was successful for 1 host |
| Duration: | 01:21:22 |
| Title: | basicvm_authenticated |
| Asset Groups: | - |
| IPs: | 192.168.0.4 |
| Excluded IPs: | - |
| Options Profile: | basicnetscan |

## Summary of Vulnerabilities

| Vulnerabilities Total | 442 |
|---|---|

| Security Risk (Avg) | 5.0 |
|---|---|

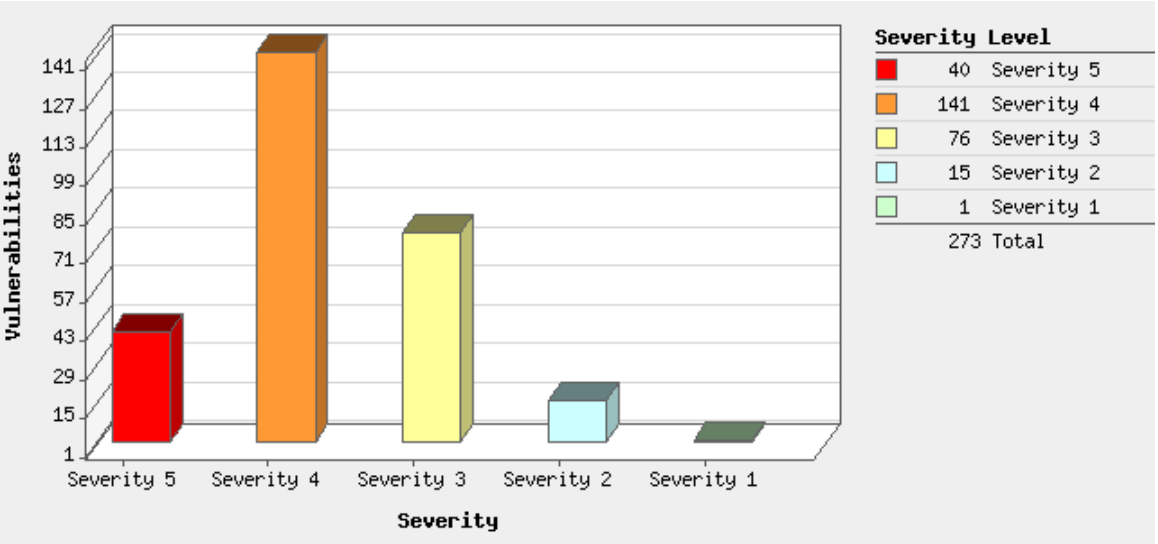
by Severity

| Severity | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| 5 | 40 | 0 | 0 | 40 |
| 4 | 141 | 0 | 0 | 141 |
| 3 | 76 | 3 | 11 | 90 |
| 2 | 15 | 2 | 51 | 68 |
| 1 | 1 | 0 | 102 | 103 |
| Total | 273 | 5 | 164 | 442 |

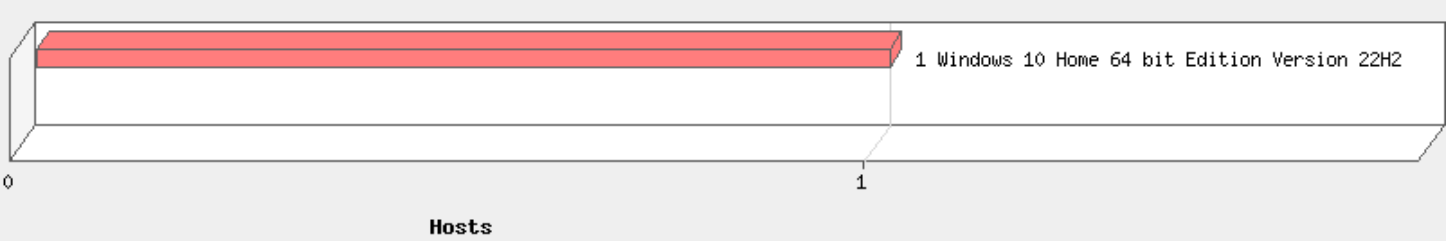
5 Biggest Categories

| Category | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| Local | 242 | 0 | 4 | 246 |
| Security Policy | 4 | 2 | 58 | 64 |
| Information gathering | 0 | 1 | 59 | 60 |
| Windows | 26 | 2 | 22 | 50 |
| TCP/IP | 0 | 0 | 7 | 7 |
| Total | 272 | 5 | 150 | 427 |

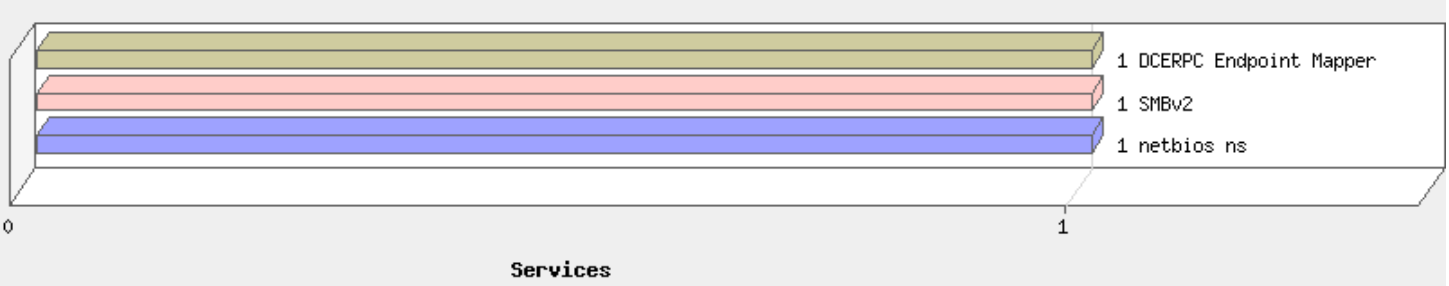
## Vulnerabilities by Severity




## Operating Systems Detected




## Services Detected




# Detailed Results

## 192.168.0.4 (win10, WIN10) Windows 10 Home 64 bit Edition Version 22H2

### Vulnerabilities (273)

5 Microsoft Windows Security Update for June 2023

QID: 92025
Category: Windows
Associated CVEs: CVE-2023-32022, CVE-2023-32021, CVE-2023-32019, CVE-2023-32018, CVE-2023-32017, CVE-2023-32016, CVE-2023-32015, CVE-2023-32014, CVE-2023-32013, CVE-2023-32012, CVE-2023-32011, CVE-2023-32010, CVE-2023-32009, CVE-2023-32008, CVE-2023-29373, CVE-2023-29372, CVE-2023-29371, CVE-2023-29370, CVE-2023-29369, CVE-2023-29368, CVE-2023-29367, CVE-2023-29366, CVE-2023-29365, CVE-2023-29364, CVE-2023-29363, CVE-2023-29362, CVE-2023-29361, CVE-2023-29360, CVE-2023-29359, CVE-2023-29358,

| | |
|---|---|
| | CVE-2023-29355, CVE-2023-29352, CVE-2023-29351, CVE-2023-29346, CVE-2023-24938, CVE-2023-24937 |
| Vendor Reference: | KB5027215, KB5027219, KB5027222, KB5027223, KB5027225, KB5027230, KB5027231, KB5027271, KB5027275, KB5027277, KB5027279, KB5027281, KB5027282, KB5027283 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - June 2023
The patch version is 6.3.9600.21013 for (https://support.microsoft.com/en-in/help/5027271)
The patch version is 6.3.9600.21013 for (https://support.microsoft.com/en-in/help/5027282)
The patch version is 10.0.14393.5989 for (https://support.microsoft.com/en-in/help/5027219)
The patch version is 10.0.20348.1787 for (https://support.microsoft.com/en-in/help/5027225)
The patch version is 10.0.17763.4499 for (https://support.microsoft.com/en-in/help/5027222)
The patch version is 6.2.9200.24312 for (https://support.microsoft.com/en-in/help/5027283)
The patch version is 6.2.9200.24312 for (https://support.microsoft.com/en-in/help/5027281)
The patch version is 6.1.7601.26561 for (https://support.microsoft.com/en-in/help/5027275)
The patch version is 6.0.6003.22112 for (https://support.microsoft.com/en-in/help/5027279)
The patch version is 6.0.6003.22112 for (https://support.microsoft.com/en-in/help/5027277)
The patch version is for (https://support.microsoft.com/en-in/help/5027215)
The patch version is 10.0.22621.1848 for (https://support.microsoft.com/en-in/help/5027231)
The patch version is 10.0.22000.2057 for (https://support.microsoft.com/en-in/help/5027223)
The patch version is 10.0.10240.19983 for (https://support.microsoft.com/en-in/help/5027230)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
(https://support.microsoft.com/en-in/help/5027271)
(https://support.microsoft.com/en-in/help/5027282)
(https://support.microsoft.com/en-in/help/5027219)
(https://support.microsoft.com/en-in/help/5027225)
(https://support.microsoft.com/en-in/help/5027222)
(https://support.microsoft.com/en-in/help/5027283)
(https://support.microsoft.com/en-in/help/5027281)
(https://support.microsoft.com/en-in/help/5027275)
(https://support.microsoft.com/en-in/help/5027279)
(https://support.microsoft.com/en-in/help/5027277)
(https://support.microsoft.com/en-in/help/5027215)
(https://support.microsoft.com/en-in/help/5027231)
(https://support.microsoft.com/en-in/help/5027223)
(https://support.microsoft.com/en-in/help/5027230)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5027271 (https://support.microsoft.com/en-in/help/5027271)
KB5027282 (https://support.microsoft.com/en-in/help/5027282)
KB5027219 (https://support.microsoft.com/en-in/help/5027219)
KB5027225 (https://support.microsoft.com/en-in/help/5027225)
KB5027222 (https://support.microsoft.com/en-in/help/5027222)
KB5027283 (https://support.microsoft.com/en-in/help/5027283)
KB5027281 (https://support.microsoft.com/en-in/help/5027281)
KB5027275 (https://support.microsoft.com/en-in/help/5027275)
KB5027279 (https://support.microsoft.com/en-in/help/5027279)
KB5027277 (https://support.microsoft.com/en-in/help/5027277)
KB5027215 (https://support.microsoft.com/en-in/help/5027215)
KB5027231 (https://support.microsoft.com/en-in/help/5027231)
KB5027223 (https://support.microsoft.com/en-in/help/5027223)
KB5027230 (https://support.microsoft.com/en-in/help/5027230)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm
Reference: CVE-2023-32019

Description: Windows Kernel KTM Registry Transactions Non-Atomic Outcomes
Link: https://packetstormsecurity.com/files/173310/Windows-Kernel-KTM-Registry-Transactions-Non-Atomic-Outcomes.html

github-exploits
Reference: CVE-2023-29360
Description: exotikcheat/cve-2023-29360 exploit repository
Link: https://github.com/exotikcheat/cve-2023-29360

Reference: CVE-2023-29360
Description: Nero22k/cve-2023-29360 exploit repository
Link: https://github.com/Nero22k/cve-2023-29360

coreimpact
Reference: CVE-2023-29360
Description: Microsoft Streaming Service Elevation of Privilege Vulnerability Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5027215 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

## 5 Microsoft Windows Security Update for August 2023

| | |
|---|---|
| QID: | 92046 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-38254, CVE-2023-38186, CVE-2023-38184, CVE-2023-38172, CVE-2023-38170, CVE-2023-38154, CVE-2023-36914, CVE-2023-36913, CVE-2023-36912, CVE-2023-36911, CVE-2023-36910, CVE-2023-36909, CVE-2023-36908, CVE-2023-36907, CVE-2023-36906, CVE-2023-36905, CVE-2023-36904, CVE-2023-36903, CVE-2023-36900, CVE-2023-36898, CVE-2023-36889, CVE-2023-36882, CVE-2023-36876, CVE-2023-35387, CVE-2023-35386, CVE-2023-35385, CVE-2023-35384, CVE-2023-35383, CVE-2023-35382, CVE-2023-35381, CVE-2023-35380, CVE-2023-35379, CVE-2023-35378, CVE-2023-35377, CVE-2023-35376, CVE-2023-35359, CVE-2023-20569 |
| Vendor Reference: | KB5029242, KB5029244, KB5029247, KB5029250, KB5029253, KB5029259, KB5029263, KB5029295, KB5029296, KB5029301, KB5029304, KB5029307, KB5029308, KB5029312, KB5029318 |
| Bugtraq ID: | - |
| Service Modified: | 12/21/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - August 2023
The patch version is 6.3.9600.21501 for 5029312 (https://support.microsoft.com/en-in/help/5029312)
The patch version is 6.3.9600.21501 for 5029304 (https://support.microsoft.com/en-in/help/5029304)
The patch version is 6.2.9200.24412 for 5029295 (https://support.microsoft.com/en-in/help/5029295)
The patch version is 6.2.9200.24412 for 5029308 (https://support.microsoft.com/en-in/help/5029308)
The patch version is 6.1.7601.26662 for 5029296 (https://support.microsoft.com/en-in/help/5029296)
The patch version is 6.1.7601.26662 for 5029307 (https://support.microsoft.com/en-in/help/5029307)
The patch version is 6.0.6003.22214 for 5029318 (https://support.microsoft.com/en-in/help/5029318)
The patch version is 6.0.6003.22214 for 5029301 (https://support.microsoft.com/en-in/help/5029301)
The patch version is 10.0.14393.6167 for 5029242 (https://support.microsoft.com/en-in/help/5029242)
The patch version is 10.0.10240.20107 for 5029259 (https://support.microsoft.com/en-in/help/5029259)
The patch version is 10.0.19041.3324 for 5029244 (https://support.microsoft.com/en-in/help/5029244)
The patch version is 10.0.22621.2134 for 5029263 (https://support.microsoft.com/en-in/help/5029263)
The patch version is 10.0.22000.2295 for 5029253 (https://support.microsoft.com/en-in/help/5029253)
The patch version is 10.0.20348.1906 for 5029250 (https://support.microsoft.com/en-in/help/5029250)
The patch version is 10.0.17763.4737 for 5029247 (https://support.microsoft.com/en-in/help/5029247)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
5029312 (https://support.microsoft.com/en-in/help/5029312)
5029304 (https://support.microsoft.com/en-in/help/5029304)
5029295 (https://support.microsoft.com/en-in/help/5029295)
5029308 (https://support.microsoft.com/en-in/help/5029308)
5029296 (https://support.microsoft.com/en-in/help/5029296)
5029307 (https://support.microsoft.com/en-in/help/5029307)
5029318 (https://support.microsoft.com/en-in/help/5029318)
5029301 (https://support.microsoft.com/en-in/help/5029301)
5029242 (https://support.microsoft.com/en-in/help/5029242)
5029259 (https://support.microsoft.com/en-in/help/5029259)
5029244 (https://support.microsoft.com/en-in/help/5029244)
5029263 (https://support.microsoft.com/en-in/help/5029263)
5029253 (https://support.microsoft.com/en-in/help/5029253)
5029250 (https://support.microsoft.com/en-in/help/5029250)
5029247 (https://support.microsoft.com/en-in/help/5029247)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5029312 (https://support.microsoft.com/en-in/help/5029312)
KB5029304 (https://support.microsoft.com/en-in/help/5029304)
KB5029295 (https://support.microsoft.com/en-in/help/5029295)
KB5029308 (https://support.microsoft.com/en-in/help/5029308)
KB5029296 (https://support.microsoft.com/en-in/help/5029296)
KB5029307 (https://support.microsoft.com/en-in/help/5029307)
KB5029318 (https://support.microsoft.com/en-in/help/5029318)
KB5029301 (https://support.microsoft.com/en-in/help/5029301)
KB5029242 (https://support.microsoft.com/en-in/help/5029242)
KB5029259 (https://support.microsoft.com/en-in/help/5029259)
KB5029244 (https://support.microsoft.com/en-in/help/5029244)
KB5029263 (https://support.microsoft.com/en-in/help/5029263)
KB5029253 (https://support.microsoft.com/en-in/help/5029253)
KB5029250 (https://support.microsoft.com/en-in/help/5029250)
KB5029247 (https://support.microsoft.com/en-in/help/5029247)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2023-35359
Description: Microsoft Windows Privilege Escalation
Link: https://packetstormsecurity.com/files/174528/Microsoft-Windows-Privilege-Escalation.html

Reference: CVE-2023-35382
Description: Microsoft Windows Kernel Use-After-Free
Link: https://packetstormsecurity.com/files/174450/Microsoft-Windows-Kernel-Use-After-Free.html

Reference: CVE-2023-35386
Description: Microsoft Windows Kernel Integer Overflow / Out-Of-Bounds Read
Link: https://packetstormsecurity.com/files/174567/Microsoft-Windows-Kernel-Integer-Overflow-Out-Of-Bounds-Read.html

Reference: CVE-2023-38154
Description: Microsoft Windows Kernel Recovery Memory Corruption
Link: https://packetstormsecurity.com/files/174568/Microsoft-Windows-Kernel-Recovery-Memory-Corruption.html

coreimpact

Reference: CVE-2023-35359
Description: Windows File History Service FHSVC Elevation of Privilege Exploit Update
Link: https://www.coresecurity.com/core-labs/exploits

blogs

Reference: CVE-2023-35359

Description: SSD Advisory - File History Service (fhsvc.dll) Elevation of Privilege
Link: https://ssd-disclosure.com/ssd-advisory-file-history-service-fhsvc-dll-elevation-of-privilege/

Reference: CVE-2023-35384
Description: Mute the Sound: Chaining Vulnerabilities to Achieve RCE on Outlook: Pt 1
Link: https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-one

nist-nvd2
Reference: CVE-2023-20569
Description: A side channel vulnerability on some of the AMD CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled?address, potentially leading to information disclosure.
Link: https://comsec.ethz.ch/research/microarch/inception/

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2023-35359
Type: Exploit
Platform: Win64

RESULTS:

KB5029244 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

5 Microsoft Windows Security Update for October 2023

QID: 92069
Category: Windows
Associated CVEs: CVE-2023-41774, CVE-2023-41773, CVE-2023-41772, CVE-2023-41771, CVE-2023-41770, CVE-2023-41769, CVE-2023-41768, CVE-2023-41767, CVE-2023-41766, CVE-2023-41765, CVE-2023-38171, CVE-2023-38166, CVE-2023-38159, CVE-2023-36902, CVE-2023-36790, CVE-2023-36776, CVE-2023-36743, CVE-2023-36732, CVE-2023-36731, CVE-2023-36729, CVE-2023-36726, CVE-2023-36725, CVE-2023-36724, CVE-2023-36723, CVE-2023-36722, CVE-2023-36721, CVE-2023-36720, CVE-2023-36718, CVE-2023-36717, CVE-2023-36713, CVE-2023-36712, CVE-2023-36711, CVE-2023-36710, CVE-2023-36709, CVE-2023-36707, CVE-2023-36706, CVE-2023-36704, CVE-2023-36703, CVE-2023-36702, CVE-2023-36701, CVE-2023-36698, CVE-2023-36697, CVE-2023-36606, CVE-2023-36605, CVE-2023-36603, CVE-2023-36602, CVE-2023-36598, CVE-2023-36596, CVE-2023-36594, CVE-2023-36593, CVE-2023-36592, CVE-2023-36591, CVE-2023-36590, CVE-2023-36589, CVE-2023-36585, CVE-2023-36584, CVE-2023-36583, CVE-2023-36582, CVE-2023-36581, CVE-2023-36579, CVE-2023-36578, CVE-2023-36577, CVE-2023-36576, CVE-2023-36575, CVE-2023-36574, CVE-2023-36573, CVE-2023-36572, CVE-2023-36571, CVE-2023-36570, CVE-2023-36567, CVE-2023-36564, CVE-2023-36563, CVE-2023-36557, CVE-2023-36438, CVE-2023-36436, CVE-2023-36435, CVE-2023-36434, CVE-2023-36431, CVE-2023-35349, CVE-2023-29348
Vendor Reference: KB5031354, KB5031356, KB5031358, KB5031361, KB5031362, KB5031364, KB5031377, KB5031407, KB5031408, KB5031411, KB5031416, KB5031419, KB5031427, KB5031441, KB5031442
Bugtraq ID: -
Service Modified: 12/21/2023
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Microsoft Windows Security Update - October 2023
Patch version is 6.3.9600.21620 for KB5031419 (https://support.microsoft.com/en-in/help/5031419)
Patch version is 6.3.9600.21620 for KB5031407 (https://support.microsoft.com/en-in/help/5031407)
Patch version is 6.2.9200.24523 for KB5031442 (https://support.microsoft.com/en-in/help/5031442)
Patch version is 6.2.9200.24523 for KB5031427 (https://support.microsoft.com/en-in/help/5031427)
Patch version is 6.1.7601.26769 for KB5031408 (https://support.microsoft.com/en-in/help/5031408)
Patch version is 6.1.7601.26769 for KB5031441 (https://support.microsoft.com/en-in/help/5031441)
Patch version is 6.0.6003.22317 for KB5031416 (https://support.microsoft.com/en-in/help/5031416)

Patch version is 6.0.6003.22317 for KB5031411 (https://support.microsoft.com/en-in/help/5031411)
Patch version is 10.0.14393.6343 for KB5031362 (https://support.microsoft.com/en-in/help/5031362)
Patch version is 10.0.10240.20232 for KB5031377 (https://support.microsoft.com/en-in/help/5031377)
Patch version is 10.0.19041.3570 for KB5031356 (https://support.microsoft.com/en-in/help/5031356)
Patch version is 10.0.22621.2428 for KB5031354 (https://support.microsoft.com/en-in/help/5031354)
Patch version is 10.0.22000.2538 for KB5031358 (https://support.microsoft.com/en-in/help/5031358)
Patch version is 10.0.20348.2031 for KB5031364 (https://support.microsoft.com/en-in/help/5031364)
Patch version is 10.0.17763.4974 for KB5031361 (https://support.microsoft.com/en-in/help/5031361)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

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

KB5031419 (https://support.microsoft.com/en-in/help/5031419)
KB5031407 (https://support.microsoft.com/en-in/help/5031407)
KB5031442 (https://support.microsoft.com/en-in/help/5031442)
KB5031427 (https://support.microsoft.com/en-in/help/5031427)
KB5031408 (https://support.microsoft.com/en-in/help/5031408)
KB5031441 (https://support.microsoft.com/en-in/help/5031441)
KB5031416 (https://support.microsoft.com/en-in/help/5031416)
KB5031411 (https://support.microsoft.com/en-in/help/5031411)
KB5031362 (https://support.microsoft.com/en-in/help/5031362)
KB5031377 (https://support.microsoft.com/en-in/help/5031377)
KB5031356 (https://support.microsoft.com/en-in/help/5031356)
KB5031354 (https://support.microsoft.com/en-in/help/5031354)
KB5031358 (https://support.microsoft.com/en-in/help/5031358)
KB5031364 (https://support.microsoft.com/en-in/help/5031364)
KB5031361 (https://support.microsoft.com/en-in/help/5031361)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5031419 (https://support.microsoft.com/en-in/help/5031419)
KB5031407 (https://support.microsoft.com/en-in/help/5031407)
KB5031442 (https://support.microsoft.com/en-in/help/5031442)
KB5031427 (https://support.microsoft.com/en-in/help/5031427)
KB5031408 (https://support.microsoft.com/en-in/help/5031408)
KB5031441 (https://support.microsoft.com/en-in/help/5031441)
KB5031416 (https://support.microsoft.com/en-in/help/5031416)
KB5031411 (https://support.microsoft.com/en-in/help/5031411)
KB5031362 (https://support.microsoft.com/en-in/help/5031362)
KB5031377 (https://support.microsoft.com/en-in/help/5031377)
KB5031356 (https://support.microsoft.com/en-in/help/5031356)
KB5031354 (https://support.microsoft.com/en-in/help/5031354)
KB5031358 (https://support.microsoft.com/en-in/help/5031358)
KB5031364 (https://support.microsoft.com/en-in/help/5031364)
KB5031361 (https://support.microsoft.com/en-in/help/5031361)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm
- Reference: CVE-2023-36576
- Description: Windows Kernel Containerized Registry Escape
- Link: https://packetstormsecurity.com/files/175659/Windows-Kernel-Containerized-Registry-Escape.html

cisa-alerts
- Reference: CVE-2023-36563
- Description: CISA Adds Five Known Vulnerabilities to Catalog
- Link: https://cisa.gov/news-events/alerts/2023/10/10/cisa-adds-five-known-vulnerabilities-catalog

github-exploits
- Reference: CVE-2023-36723
- Description: Wh04m1001/CVE-2023-36723 exploit repository
- Link: https://github.com/Wh04m1001/CVE-2023-36723

cisa-kev
- Reference: CVE-2023-36563

Description: Microsoft WordPad Information Disclosure Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2023-36584
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-2023-36584
Description: In-Depth Analysis of July 2023 Exploit Chain Featuring CVE-2023-36884 and CVE-2023-36584
Link: https://unit42.paloaltonetworks.com/new-cve-2023-36584-discovered-in-attack-chain-used-by-russian-apt/

Reference: CVE-2023-36710
Description: Mute the Sound: Chaining Vulnerabilities to Achieve RCE on Outlook: Pt 1
Link: https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-one

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2023-36584
Type: Exploit
Platform: Script

RESULTS:

KB5031356 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

5 Microsoft Windows Security Update for November 2023

| | |
|---|---|
| QID: | 92075 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-36017, CVE-2023-36025, CVE-2023-36398, CVE-2023-36036, CVE-2023-36399, CVE-2023-36394, CVE-2023-36424, CVE-2023-36393, CVE-2023-36028, CVE-2023-36396, CVE-2023-36719, CVE-2023-36403, CVE-2023-36423, CVE-2023-36046, CVE-2023-36406, CVE-2023-36407, CVE-2023-36392, CVE-2023-36427, CVE-2023-36404, CVE-2023-36395, CVE-2023-36408, CVE-2023-36047, CVE-2023-24023, CVE-2023-36405, CVE-2023-36400, CVE-2023-36705, CVE-2023-36401, CVE-2023-36428, CVE-2023-36402, CVE-2023-36425, CVE-2023-36397, CVE-2023-36033 |
| Vendor Reference: | KB5032189, KB5032190, KB5032192, KB5032196, KB5032197, KB5032198, KB5032199, KB5032247, KB5032248, KB5032249, KB5032250, KB5032252, KB5032254 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - November 2023
Patch version is 10.0.22621.2715 for KB5032190 (https://support.microsoft.com/en-in/help/5032190)
Patch version is 6.3.9600.21662 for KB5032249 (https://support.microsoft.com/en-in/help/5032249)
Patch version is 6.2.9200.24565 for KB5032247 (https://support.microsoft.com/en-in/help/5032247)
Patch version is 6.1.7601.26812 for KB5032252 (https://support.microsoft.com/en-in/help/5032252)
Patch version is 6.1.7601.26812 for KB5032250 (https://support.microsoft.com/en-in/help/5032250)
Patch version is 6.0.6003.22366 for KB5032254 (https://support.microsoft.com/en-in/help/5032254)
Patch version is 6.0.6003.22366 for KB5032248 (https://support.microsoft.com/en-in/help/5032248)
Patch version is 10.0.14393.6451 for KB5032197 (https://support.microsoft.com/en-in/help/5032197)
Patch version is 10.0.10240.20307 for KB5032199 (https://support.microsoft.com/en-in/help/5032199)
Patch version is 10.0.19041.3693 for KB5032189 (https://support.microsoft.com/en-in/help/5032189)
Patch version is 10.0.22000.2600 for KB5032192 (https://support.microsoft.com/en-in/help/5032192)
Patch version is 10.0.20348.2110 for KB5032198 (https://support.microsoft.com/en-in/help/5032198)
Patch version is 10.0.17763.5122 for KB5032196 (https://support.microsoft.com/en-in/help/5032196)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

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

Patch version is 10.0.22621.2715 for KB5032190 (https://support.microsoft.com/en-in/help/5032190)
Patch version is 6.3.9600.21662 for KB5032249 (https://support.microsoft.com/en-in/help/5032249)
Patch version is 6.2.9200.24565 for KB5032247 (https://support.microsoft.com/en-in/help/5032247)
Patch version is 6.1.7601.26812 for KB5032252 (https://support.microsoft.com/en-in/help/5032252)
Patch version is 6.1.7601.26812 for KB5032250 (https://support.microsoft.com/en-in/help/5032250)
Patch version is 6.0.6003.22366 for KB5032254 (https://support.microsoft.com/en-in/help/5032254)
Patch version is 6.0.6003.22366 for KB5032248 (https://support.microsoft.com/en-in/help/5032248)
Patch version is 10.0.14393.6451 for KB5032197 (https://support.microsoft.com/en-in/help/5032197)
Patch version is 10.0.10240.20307 for KB5032199 (https://support.microsoft.com/en-in/help/5032199)
Patch version is 10.0.19041.3693 for KB5032189 (https://support.microsoft.com/en-in/help/5032189)
Patch version is 10.0.22000.2600 for KB5032192 (https://support.microsoft.com/en-in/help/5032192)
Patch version is 10.0.20348.2110 for KB5032198 (https://support.microsoft.com/en-in/help/5032198)
Patch version is 10.0.17763.5122 for KB5032196 (https://support.microsoft.com/en-in/help/5032196)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5032190 (https://support.microsoft.com/en-in/help/5032190)
KB5032249 (https://support.microsoft.com/en-in/help/5032249)
KB5032247 (https://support.microsoft.com/en-in/help/5032247)
KB5032252 (https://support.microsoft.com/en-in/help/5032252)
KB5032250 (https://support.microsoft.com/en-in/help/5032250)
KB5032254 (https://support.microsoft.com/en-in/help/5032254)
KB5032248 (https://support.microsoft.com/en-in/help/5032248)
KB5032197 (https://support.microsoft.com/en-in/help/5032197)
KB5032199 (https://support.microsoft.com/en-in/help/5032199)
KB5032189 (https://support.microsoft.com/en-in/help/5032189)
KB5032192 (https://support.microsoft.com/en-in/help/5032192)
KB5032198 (https://support.microsoft.com/en-in/help/5032198)
KB5032196 (https://support.microsoft.com/en-in/help/5032196)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2023-36404
Description: Windows Kernel Information Disclosure
Link: https://packetstormsecurity.com/files/176110/Windows-Kernel-Information-Disclosure.html

Reference: CVE-2023-36403
Description: Windows Kernel Race Conditions
Link: https://packetstormsecurity.com/files/176209/Windows-Kernel-Race-Conditions.html

github-exploits

Reference: CVE-2023-36427
Description: tandasat/CVE-2023-36427 exploit repository
Link: https://github.com/tandasat/CVE-2023-36427

cisa-kev

Reference: CVE-2023-36025
Description: Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2023-36033
Description: Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2023-36036
Description: Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2023-36033

Description: Microsoft Windows DWM Core Library Elevation of Privilege
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2023-36036
Description: Microsoft Windows Cloud Files Mini Filter Driver Elevation of Privilege
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5032189 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

### 5 Microsoft Windows Security Update for December 2023

| | |
|---|---|
| QID: | 92085 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-36696, CVE-2023-36391, CVE-2023-36011, CVE-2023-36006, CVE-2023-36005, CVE-2023-36004, CVE-2023-36003, CVE-2023-35644, CVE-2023-35642, CVE-2023-35641, CVE-2023-35639, CVE-2023-35635, CVE-2023-35634, CVE-2023-35633, CVE-2023-35632, CVE-2023-35631, CVE-2023-35630, CVE-2023-35629, CVE-2023-35628, CVE-2023-21740, CVE-2023-20588 |
| Vendor Reference: | KB5033118, KB5033369, KB5033371, KB5033372, KB5033373, KB5033375, KB5033379, KB5033383, KB5033422, KB5033424, KB5033427, KB5033429, KB5033433 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - December 2023
Patch version is 10.0.22621.2861 for KB5033375 (https://support.microsoft.com/en-in/help/5033375)
Patch version is 10.0.25398.584 for KB5033383 (https://support.microsoft.com/en-in/help/5033383)
Patch version is 10.0.19041.3803 for KB5033372 (https://support.microsoft.com/en-in/help/5033372)
Patch version is 10.0.22000.2652 for KB5033369 (https://support.microsoft.com/en-in/help/5033369)
Patch version is 10.0.20348.2141 for KB5033118 (https://support.microsoft.com/en-in/help/5033118)
Patch version is 10.0.17763.5202 for KB5033371 (https://support.microsoft.com/en-in/help/5033371)
Patch version is 6.2.9200.24612 for KB5033429 (https://support.microsoft.com/en-in/help/5033429)
Patch version is 6.1.7601.26863 for KB5033433 (https://support.microsoft.com/en-in/help/5033433)
Patch version is 6.1.7601.26863 for KB5033424 (https://support.microsoft.com/en-in/help/5033424)
Patch version is 6.0.6003.22412 for KB5033422 (https://support.microsoft.com/en-in/help/5033422)
Patch version is 6.0.6003.22412 for KB5033427 (https://support.microsoft.com/en-in/help/5033427)
Patch version is 10.0.14393.6522 for KB5033373 (https://support.microsoft.com/en-in/help/5033373)
Patch version is 10.0.10240.20345 for KB5033379 (https://support.microsoft.com/en-in/help/5033379)
Patch version is 6.3.9600.21712 for KB5033420 (https://support.microsoft.com/en-in/help/5033379)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

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

KB5033375 (https://support.microsoft.com/en-in/help/5033375)
KB5033383 (https://support.microsoft.com/en-in/help/5033383)
KB5033372 (https://support.microsoft.com/en-in/help/5033372)
KB5033369 (https://support.microsoft.com/en-in/help/5033369)
KB5033118 (https://support.microsoft.com/en-in/help/5033118)
KB5033464 (https://support.microsoft.com/en-in/help/5033464)
KB5033371 (https://support.microsoft.com/en-in/help/5033371)
KB5033429 (https://support.microsoft.com/en-in/help/5033429)

KB5033433 (https://support.microsoft.com/en-in/help/5033433)
KB5033424 (https://support.microsoft.com/en-in/help/5033424)
KB5033422 (https://support.microsoft.com/en-in/help/5033422)
KB5033427 (https://support.microsoft.com/en-in/help/5033427)
KB5033373 (https://support.microsoft.com/en-in/help/5033373)
KB5033379 (https://support.microsoft.com/en-in/help/5033379)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5033375 (https://support.microsoft.com/en-in/help/5033375)
KB5033383 (https://support.microsoft.com/en-in/help/5033383)
KB5033372 (https://support.microsoft.com/en-in/help/5033372)
KB5033369 (https://support.microsoft.com/en-in/help/5033369)
KB5033118 (https://support.microsoft.com/en-in/help/5033118)
KB5033371 (https://support.microsoft.com/en-in/help/5033371)
KB5033429 (https://support.microsoft.com/en-in/help/5033429)
KB5033433 (https://support.microsoft.com/en-in/help/5033433)
KB5033424 (https://support.microsoft.com/en-in/help/5033424)
KB5033422 (https://support.microsoft.com/en-in/help/5033422)
KB5033427 (https://support.microsoft.com/en-in/help/5033427)
KB5033373 (https://support.microsoft.com/en-in/help/5033373)
KB5033379 (https://support.microsoft.com/en-in/help/5033379)
KB5033420 (https://support.microsoft.com/en-in/help/5033420)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5033372 is not installed
%windir%\system32\ntoskrnl.exe  Version is  10.0.19041.2965

### 5 EOL/Obsolete Software: Mozilla Firefox Prior to 81 Detected

| | |
|---|---|
| QID: | 105444 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | Firefox End of Life |
| Bugtraq ID: | - |
| Service Modified: | 09/06/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a free and open source web browser that uses the Gecko layout engine to render web pages, which implements current and anticipated web standards.
The current stable release for Mozilla Firefox is version 81, that was released on October 2, 2020.

IMPACT:

Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks exposing the system to security vulnerabilities.

SOLUTION:

Upgrade to the latest version of Mozilla Firefox from the Mozilla Project (http://www.mozilla.org/) website.

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  1.7.0.0

### 5 EOL/Obsolete Software: Mozilla Firefox 1.x Detected

| | |
|---|---|
| QID: | 105446 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 09/06/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox 1.x has reached product End of Life in its support cycle.
No further bug fixes, enhancements, security updates or technical support is available for this version.

IMPACT:

The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:

Upgrade a supported version of Mozilla Firefox.
Supported versions can be found at  Mozilla Project (http://www.mozilla.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)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 5 Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA 2011-01 through MFSA 2011-10)

| | |
|---|---|
| QID: | 119017 |
| Category: | Local |
| Associated CVEs: | CVE-2010-1585, CVE-2011-0051, CVE-2011-0053, CVE-2011-0054, CVE-2011-0055, CVE-2011-0056, CVE-2011-0057, CVE-2011-0058, CVE-2011-0059, CVE-2011-0061, CVE-2011-0062 |
| Vendor Reference: | mfsa2011-07, mfsa2011-01, mfsa2011-02, mfsa2011-03, mfsa2011-04, mfsa2011-05, mfsa2011-06, mfsa2011-08, mfsa2011-09, mfsa2011-10 |
| Bugtraq ID: | 46645,46648,46661,46650,46663,46660,46652,46651,46647 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client. SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to the following vulnerabilities:
1) Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
2) An error when handling recursive calls to "eval()" within a "try/catch" statement can lead to dialogs being displayed incorrectly and returning "true" when being closed. This can e.g. be exploited to gain escalated privileges by forcing a user into accepting certain dialogs.
3) A use-after-free error in the js3250.dll library when processing the "JSON.stringify()" method can be exploited to dereference an invalid pointer in a call to the "js_HasOwnProperty()" function.
4) An error within the internal memory mapping of non-local JavaScript variables can be exploited to cause a buffer overflow and potentially execute arbitrary code.
5) An error within the internal string mapping of the JavaScript engine related to an offset pointer when handling more than 64K values can be exploited to cause an exception object to be read from invalid memory.
6) A use-after-free error related to JavaScript "Workers" can be exploited to dereference invalid memory and execute arbitrary code.
7) An error when allocating memory for layout objects displaying long strings can be exploited to cause a memory corruption and execute arbitrary code.
Note: This may only affect the Windows platform.
8) The "ParanoidFragmentSink" class does not properly filter "javascript:" URLs and inline JavaScript, which can be exploited to execute arbitrary JavaScript code.
Successful exploitation requires that an extension using the function to sanitize HTML code before embedding it in a chrome document is installed.
9) An error when decoding certain JPEG images can be exploited to cause a buffer overflow and potentially execute arbitrary code.
10) When a request initiated by the plugin received a redirect response (307), the request including any custom headers is incorrectly forwarded to the new location without notifying the plugin, which can be used to e.g. bypass cross-site request forgery protections relying on custom headers.
Affected Versions:
Firefox prior to 3.5.17, Firefox 3.6.x prior to 3.6.14, Thunderbird prior to 3.1.8, SeaMonkey prior to 2.0.12.

IMPACT:

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

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2011-01 (http://www.mozilla.org/security/announce/2011/mfsa2011-01.html), MFSA 2011-02 (http://www.mozilla.org/security/announce/2011/mfsa2011-02.html), MFSA2011-03 (http://www.mozilla.org/security/announce/2011/mfsa2011-03.html), MFSA2011-04 (http://www.mozilla.org/security/announce/2011/mfsa2011-04.html), MFSA2011-05 (http://www.mozilla.org/security/announce/2011/mfsa2011-05.html), MFSA2011-06 (http://www.mozilla.org/security/announce/2011/mfsa2011-06.html), MFSA2011-07 (http://www.mozilla.org/security/announce/2011/mfsa2011-07.html), MFSA2011-08 (http://www.mozilla.org/security/announce/2011/mfsa2011-08.html), MFSA2011-09 (http://www.mozilla.org/security/announce/2011/mfsa2011-09.html) and MFSA2011-10 (http://www.mozilla.org/security/announce/2011/mfsa2011-10.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2011-01 through MFSA 2011-10: Linux (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.14&os=linux&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.12&os=linux&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Linux (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.8&os=linux&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Linux (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.17&os=linux&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Mac OS (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.8&os=osx&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Mac OS (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.14&os=osx&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Mac OS (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.12&os=osx&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Mac OS (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.17&os=win&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Windows (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.14&os=win&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Windows (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.17&os=win&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.12&os=win&lang=en-US)
MFSA 2011-01 through MFSA 2011-10: Windows (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.8&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2010-1585

Description: The nsIScriptableUnescapeHTML.parseFragment method in the ParanoidFragmentSink protection mechanism in Mozilla Firefox before 3.5.17 and 3.6.x before 3.6.14, Thunderbird before 3.1.8, and SeaMonkey before 2.0.12 does not properly sanitize HTML in a chrome document, which makes it easier for remote attackers to execute arbitrary JavaScript with chrome privileges via a javascript: URI in input to an extension, as demonstrated by a javascript:alert sequence in (1) the HREF

attribute of an A element

Link: http://www.security-assessment.com/files/whitepapers/Cross_Context_Scripting_with_Firefox.pdf

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 5 Mozilla Firefox/SeaMonkey/Thunderbird Multiple Vulnerabilities (MFSA 2013-01 through MFSA 2013-20)

| | |
|---|---|
| QID: | 120809 |
| Category: | Local |
| Associated CVEs: | CVE-2012-5829, CVE-2013-0744, CVE-2013-0745, CVE-2013-0746, CVE-2013-0747, CVE-2013-0748, CVE-2013-0749, CVE-2013-0750, CVE-2013-0752, CVE-2013-0753, CVE-2013-0754, CVE-2013-0755, CVE-2013-0756, CVE-2013-0757, CVE-2013-0758, CVE-2013-0759, CVE-2013-0760, CVE-2013-0761, CVE-2013-0762, CVE-2013-0763, CVE-2013-0764, CVE-2013-0766, CVE-2013-0768, CVE-2013-0769, CVE-2013-0770, CVE-2013-0771, CVE-2013-0767, CVE-2013-0751 |
| Vendor Reference: | MFSA2013-01, MFSA2013-02, MFSA2013-03, MFSA2013-04, MFSA2013-05, MFSA2013-06, MFSA2013-07, MFSA2013-08, MFSA2013-09, MFSA2013-10, MFSA2013-11, MFSA2013-12, MFSA2013-13, MFSA2013-14, MFSA2013-15, MFSA2013-16, MFSA2013-17, MFSA2013-18, MFSA2013-19, MFSA2013-20 |
| Bugtraq ID: | 56636,57193,57194 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
Several unspecified errors in the browser engine can be exploited to corrupt memory.
An error within the "CharDistributionAnalysis::HandleOneChar()" function can be exploited to cause a buffer overflow.
A use-after-free error exists within the "imgRequest::OnStopFrame()" function.
A use-after-free error exists within "nsHTMLEditRules" function.
A use-after-free error exists within the "mozilla::TrackUnionStream::EndTrack()" function.
A use-after-free error exists within Mesa when resizing a WebGL canvas.
An error within the "gfxTextRun::ShrinkToLigatureBoundaries()" function.
An error within the "nsWindow::OnExposeEvent()" function.
An error when parsing height and width values of a canvas element can be exploited to cause a stack-based buffer overflow.
An error exists which can be exploited to spoof the URL displayed in the address bar while the page is loading.
A use-after-free error exists when displaying a table with many columns and column groups.
An error exists within the "nsSOCKSSocketInfo::ConnectToProxy()" function when handling SSL connection threads.
An error exists due to the "AutoWrapperChanger" class not keeping certain objects alive during garbage collection.
An error related to quickstubs can be exploited to cause a compartment mismatch and may cause the garbage collection to occur incorrectly.
An error related to events in the plugin handler can be exploited to bypass the same origin policy.
An error within the "XBL.__proto__.toString()" function can be exploited to disclose the address space layout.
An integer overflow error when calculating the length of a JavaScript string concatenation can be exploited to cause a heap-based buffer overflow.
An error related to XBL files containing multiple XML bindings with SVG content can be exploited to corrupt memory.
An error within the "Object.prototype.__proto__()" function can be exploited to bypass Chrome Object Wrappers (COW) and gain access to chrome privileged functions.
An error related to plugin objects can be exploited to open a chrome privileged web page.
A use-after-free error exists within the "XMLSerializer.serializeToStream()".
A use-after-free error exists within the ListenerManager when garbage collection is forced on certain data allocated in listener objects.
A use-after-free error exists within the Vibrate library related to the domDoc pointer.
A use-after-free error exists in the JavaScript Proxy class within the "obj_toSource()" function.
Affected Versions:
Firefox prior to18.0
Firefox ESR prior to 10.0.12
Firefox ESR prior to17.0.2
Thunderbird prior to 17.0.2
Thunderbird ESR prior to 10.0.12
Thunderbird ESR prior to 17.0.2
SeaMonkey prior to 2.15

IMPACT:

If this vulnerability is successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2013-01 (http://www.mozilla.org/security/announce/2013/mfsa2013-01.html), MFSA 2013-02 (http://www.mozilla.org/security/announce/2013/mfsa2013-02.html), MFSA2013-03 (http://www.mozilla.org/security/announce/2013/mfsa2013-03.html), MFSA2013-04 (http://www.mozilla.org/security/announce/2013/mfsa2013-04.html), MFSA2013-05 (http://www.mozilla.org/security/announce/2013/mfsa2013-05.html), MFSA2013-06 (http://www.mozilla.org/security/announce/2013/mfsa2013-06.html), MFSA2013-07 (http://www.mozilla.org/security/announce/2013/mfsa2013-07.html), MFSA2013-08 (http://www.mozilla.org/security/announce/2013/mfsa2013-08.html), MFSA2013-09 (http://www.mozilla.org/security/announce/2013/mfsa2013-09.html), MFSA2013-10 (http://www.mozilla.org/security/announce/2013/mfsa2013-10.html), MFSA2013-11 (http://www.mozilla.org/security/announce/2013/mfsa2013-11.html), MFSA2013-12 (http://www.mozilla.org/security/announce/2013/mfsa2013-12.html), MFSA2013-13 (http://www.mozilla.org/security/announce/2013/mfsa2013-13.html), MFSA2013-14 (http://www.mozilla.org/security/announce/2013/mfsa2013-14.html), MFSA2013-15 (http://www.mozilla.org/security/announce/2013/mfsa2013-15.html), MFSA2013-16 (http://www.mozilla.org/security/announce/2013/mfsa2013-16.html), MFSA2013-17 (http://www.mozilla.org/security/announce/2013/mfsa2013-17.html), MFSA2013-18 (http://www.mozilla.org/security/announce/2013/mfsa2013-18.html), MFSA2013-19 (http://www.mozilla.org/security/announce/2013/mfsa2013-19.html), MFSA2013-20 (http://www.mozilla.org/security/announce/2013/mfsa2013-20.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 18.0: Mac (download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/18.0/mac/en-US/Firefox%2018.0.dmg)
Firefox 18.0: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/18.0/win32/en-US/Firefox%20Setup%2018.0.exe)
Firefox ESR 10.0.12: Mac (http://download.mozilla.org/?product=firefox-10.0.12esr&os=osx&lang=en-US)
Firefox ESR 10.0.12: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/10.0.12esr/win32/en-US/Firefox%20Setup%2010.0.12esr.exe)
SeaMonkey: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.15/mac/en-US/SeaMonkey%202.15.dmg)
SeaMonkey: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.15/win32/en-US/SeaMonkey%20Setup%202.15.exe)
Thunderbird ESR 10.0.12: Mac (http://download.mozilla.org/?product=thunderbird-10.0.12esr&os=osx&lang=en-US)
Thunderbird ESR 10.0.12: Windows (http://download.mozilla.org/?product=thunderbird-10.0.12esr&os=win&lang=en-US)
Thunderbird 17.0.2: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.2/mac/en-US/Thunderbird%2017.0.2.dmg)
Thunderbird 17.0.2: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.2/win32/en-US/Thunderbird%20Setup%2017.0.2.exe)
Thunderbird ESR 17.0.2: Mac (http://download.mozilla.org/?product=thunderbird-17.0.2esr&os=osx&lang=en-US)
Thunderbird ESR 17.0.2: Windows (http://download.mozilla.org/?product=thunderbird-17.0.2esr&os=win&lang=en-US)
Firefox ESR 17.0.2: Mac (http://download.mozilla.org/?product=firefox-17.0.2esr&os=osx&lang=en-US)
Firefox ESR 17.0.2: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.2esr/win32/en-US/Firefox%20Setup%2017.0.2esr.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2013-0758
Description: Mozilla Firefox plugin objects Privileged Code Execution Exploit - Core Security Category : Exploits/Client Side

Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free Exploit - Core Security Category : Exploits/Client Side

Metasploit

Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free - Metasploit Ref : /modules/exploit/windows/browser/mozilla_firefox_xmlserializer
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_firefox_xmlserializer.rb

Reference: CVE-2013-0758
Description: Firefox 17.0.1 Flash Privileged Code Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_svg_plugin
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_svg_plugin.rb

Reference: CVE-2013-0757
Description: Firefox 17.0.1 Flash Privileged Code Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_svg_plugin
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_svg_plugin.rb

The Exploit-DB

Reference: CVE-2013-0758
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection (Metasploit) - The Exploit-DB Ref : 41683
Link: http://www.exploit-db.com/exploits/41683

Reference: CVE-2013-0757
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection (Metasploit) - The Exploit-DB Ref : 41683
Link: http://www.exploit-db.com/exploits/41683

Reference: CVE-2013-0758
Description: GIT 1.8.5.6/1.9.5/2.0.5/2.1.4/2.2.1 & Mercurial < 3.2.3 - Multiple Vulnerabilities (Metasploit) - The Exploit-DB Ref : 41684
Link: http://www.exploit-db.com/exploits/41684

Reference: CVE-2013-0757
Description: GIT 1.8.5.6/1.9.5/2.0.5/2.1.4/2.2.1 & Mercurial < 3.2.3 - Multiple Vulnerabilities (Metasploit) - The Exploit-DB Ref : 41684
Link: http://www.exploit-db.com/exploits/41684

Reference: CVE-2013-0753
Description: Mozilla Firefox - XMLSerializer Use-After-Free (Metasploit) - The Exploit-DB Ref : 27940
Link: http://www.exploit-db.com/exploits/27940

exploitdb

Reference: CVE-2013-0757
Description: GIT 1.8.5.6/1.9.5/2.0.5/2.1.4/2.2.1 & Mercurial < 3.2.3 - Multiple Vulnerabilities (Metasploit)
Link: https://www.exploit-db.com/exploits/41684

Reference: CVE-2013-0758
Description: GIT 1.8.5.6/1.9.5/2.0.5/2.1.4/2.2.1 & Mercurial < 3.2.3 - Multiple Vulnerabilities (Metasploit)
Link: https://www.exploit-db.com/exploits/41684

Reference: CVE-2013-0753
Description: Mozilla Firefox - XMLSerializer Use-After-Free (Metasploit)
Link: https://www.exploit-db.com/exploits/27940

Reference: CVE-2013-0757
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/41683

Reference: CVE-2013-0758
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/41683

nvd

Reference: CVE-2012-5829
Description: Heap-based buffer overflow in the nsWindow::OnExposeEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=792305

Reference: CVE-2013-0747
Description: The gPluginHandler.handleEvent function in the plugin handler in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not properly enforce the Same Origin Policy, which allows remote attackers to conduct clickjacking attacks via crafted JavaScript code that listens for a mutation event.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=733305

Reference: CVE-2013-0748
Description: The XBL.__proto__.toString implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 makes it easier for remote attackers to bypass the ASLR protection mechanism by calling the toString function of an XBL object.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=806031

Reference: CVE-2013-0749

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=805814

Reference: CVE-2013-0749

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=805745

Reference: CVE-2013-0752

Description: Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XBL file with multiple bindings that have SVG content.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=805024

Reference: CVE-2013-0755

Description: Use-after-free vulnerability in the mozVibrate implementation in the Vibrate library in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via vectors related to the domDoc pointer.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=814027

Reference: CVE-2013-0757

Description: The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not prevent modifications to the prototype of an object, which allows remote attackers to execute arbitrary JavaScript code with chrome privileges by referencing Object.prototype.__proto__ in a crafted HTML document.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=813901

Reference: CVE-2013-0759

Description: Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to spoof the address bar via vectors involving authentication information in the userinfo field of a URL, in conjunction with a 204 (aka No Content) HTTP status code.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=802026

Reference: CVE-2013-0768

Description: Stack-based buffer overflow in the Canvas implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via an HTML document that specifies invalid width and height values.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=815795

Reference: CVE-2013-0769

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=809064

Reference: CVE-2013-0769

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=801195

Reference: CVE-2013-0769

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=806483

Reference: CVE-2013-0770

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Thunderbird before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or

possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=768750

seebug
Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free
Link: https://www.seebug.org/vuldb/ssvid-81527

saint
Reference: CVE-2013-0753
Description: Mozilla Firefox XMLSerializer serializeToStream Use-after-free Vulnerability
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_xmlserializer_serializetostream_uaf

packetstorm
Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free
Link: https://packetstormsecurity.com/files/123000/Firefox-XMLSerializer-Use-After-Free.html

metasploit
Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2013-0757
Description: Firefox 17.0.1 Flash Privileged Code Injection
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2013-0758
Description: Firefox 17.0.1 Flash Privileged Code Injection
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/mozilla_firefox_xmlserializ

Reference: CVE-2013-0757
Description: Firefox 17.0.1 Flash Privileged Code Injection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_svg_plugin.rb

Reference: CVE-2013-0758
Description: Firefox 17.0.1 Flash Privileged Code Injection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_svg_plugin.rb

0day.today
Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free Vulnerability
Link: https://0day.today/exploit/21177

Reference: CVE-2013-0757
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection Exploit
Link: https://0day.today/exploit/27388

Reference: CVE-2013-0757
Description: GIT 1.8.5.6 / 1.9.5 / 2.0.5 / 2.1.4/ 2.2.1 & Mercurial < 3.2.3 - Exploit
Link: https://0day.today/exploit/27392

Reference: CVE-2013-0758
Description: Mozilla Firefox < 17.0.1 - Flash Privileged Code Injection Exploit
Link: https://0day.today/exploit/27388

Reference: CVE-2013-0758
Description: GIT 1.8.5.6 / 1.9.5 / 2.0.5 / 2.1.4/ 2.2.1 & Mercurial < 3.2.3 - Exploit
Link: https://0day.today/exploit/27392

coreimpact

Reference: CVE-2013-0753
Description: Firefox XMLSerializer Use After Free Exploit
Link: https://www.coresecurity.com/core-labs/exploits

Reference: CVE-2013-0758
Description: Mozilla Firefox plugin objects Privileged Code Execution Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: MetaSploit
Type: Hacktool
Platform: Script

Malware ID: HeapLib
Type: Trojan
Platform: Script

Malware ID: Heuristic
Type: Trojan
Platform: Script

Malware ID: CVE-2013-0753
Type: Exploit
Platform: Script

Malware ID: CVE-2012-4969
Type: Exploit
Platform: Document

Malware ID: Heuristic
Type: Exploit
Platform: Script

Malware ID: CVE-2013-0758
Type: Exploit
Platform: ByteCode,Script

Malware ID: Generic
Type: Exploit
Platform: Script

Malware ID: CVE-2013-0758
Type: Exploit
Platform: ByteCode,Win32,Script,Document

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 5 Mozilla Firefox/SeaMonkey/Thunderbird Multiple Vulnerabilities (MFSA 2013-21 through MFSA 2013-28)

| | |
|---|---|
| QID: | 120896 |
| Category: | Local |
| Associated CVEs: | CVE-2013-0783, CVE-2013-0784, CVE-2013-0772, CVE-2013-0765, CVE-2013-0773, CVE-2013-0774, CVE-2013-0775, CVE-2013-0776, CVE-2013-0777, CVE-2013-0778, CVE-2013-0779, CVE-2013-0780, CVE-2013-0781, CVE-2013-0782 |
| Vendor Reference: | mfsa2013-21.html, mfsa2013-22.html, mfsa2013-23.html, mfsa2013-24.html, mfsa2013-25.html, mfsa2013-26.html, mfsa2013-27.html, mfsa2013-28.html |
| Bugtraq ID: | - |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
1) Several memory-corruption vulnerabilities because of an unspecified error in the browser engine.
2) A remote code execution vulnerability because the applications allow bypassing certain protections in Chrome Object Wrappers (COW) and System Only Wrappers (SOW).
3) A security vulnerability that exists due to out-of-bounds read condition in the 'mozilla::image::RasterImage::DrawFrameTo()' function when processing GIF format images.
4) An information disclosure vulnerability. Specifically, this issue occurs because the file system location of the active browser profile is available to JavaScript workers.
5) A remote code execution vulnerability. Specifically, this issue occurs because the wrapped WebIDL objects can be wrapped multiple times which may result in overwriting the existing wrapped state.
6) A remote code execution vulnerability because of a heap-based buffer-overflow in the 'nsSaveAsCharset::DoCharsetConversion()' function.
7) A remote code execution vulnerability because of an out-of-bounds read in the 'ClusterIterator::NextCluster()' function.
8) An URI-spoofing vulnerability because the issue exists related to phishing on HTTPS connections through a malicious proxy.
9) A remote code execution vulnerability because of a use-after-free condition in the 'nsDisplayBoxShadowOuter::Paint()' function.
10) A remote code execution vulnerability because of a use-after-free condition in the 'nsOverflowContinuationTracker::Finish()' function.
11) A remote code execution vulnerability because of a use-after-free condition in the 'nsPrintEngine::CommonPrint()' function.
12) A remote code execution vulnerability because of an out-of-bounds read in the 'nsCodingStateMachine::NextState()' function.
13) A remote-code-execution vulnerability due to use-after-free condition. Specifically, this issue occurs in the 'nsImageLoadingContent::OnStopContainer()' function when content script is executed.
Affected Versions:
Firefox prior to19.0
Firefox ESR prior to17.0.3
Thunderbird prior to 17.0.3
Thunderbird ESR  prior to 17.0.3
SeaMonkey prior to 2.16

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to mfsa2013-22 (http://www.mozilla.org/security/announce/2013/mfsa2013-22.html), mfsa2013-23 (http://www.mozilla.org/security/announce/2013/mfsa2013-23.html), mfsa2013-24 (http://www.mozilla.org/security/announce/2013/mfsa2013-24.html), mfsa2013-25 (http://www.mozilla.org/security/announce/2013/mfsa2013-25.html), mfsa2013-26 (http://www.mozilla.org/security/announce/2013/mfsa2013-26.html), mfsa2013-27 (http://www.mozilla.org/security/announce/2013/mfsa2013-27.html), mfsa2013-28 (http://www.mozilla.org/security/announce/2013/mfsa2013-28.html) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 19: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/19.0/win32/en-US/Firefox%20Setup%2019.0.exe)
Firefox 19: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/19.0/mac/en-US/Firefox%2019.0.dmg)
Firefox 17.0.3esr: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.3esr/win32/en-US/Firefox%20Setup%2017.0.3esr.exe)
Firefox 17.0.3esr: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.3esr/mac/en-US/Firefox%2017.0.3esr.dmg)
SeaMonkey 2.16: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.16/win32/en-US/SeaMonkey%20Setup%202.16.exe)
SeaMonkey 2.16: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.16/mac/en-US/SeaMonkey%202.16.dmg)
Thunderbird 17.0.3: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.3/win32/en-US/Thunderbird%20Setup%2017.0.3.exe)
Thunderbird 17.0.3: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.3/mac/en-US/Thunderbird%2017.0.3.dmg)
Thunderbird 17.0.3esr: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.3esr/win32/en-US/Thunderbird%20Setup%2017.0.3esr.exe)
Thunderbird 17.0.3esr: Mac

(http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.3esr/mac/en-US/Thunderbird%2017.0.3esr.dmg)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2013-0774
Description: Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 do not prevent JavaScript workers from reading the browser-profile directory name, which has unspecified impact and remote attack vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=827193

Reference: CVE-2013-0777
Description: Use-after-free vulnerability in the nsDisplayBoxShadowOuter::Paint function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=798691

Reference: CVE-2013-0779
Description: The nsCodingStateMachine::NextState function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=801330

Reference: CVE-2013-0784
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=799907

Reference: CVE-2013-0784
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=819635

Reference: CVE-2013-0784
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=799803

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox/Thunderbird Multiple Vulnerabilities (MFSA 2013-49 through MFSA 2013-62)

| | |
|---|---|
| QID: | 121297 |
| Category: | Local |
| Associated CVEs: | CVE-2013-1700, CVE-2013-1699, CVE-2013-1698, CVE-2013-1697, CVE-2013-1696, CVE-2013-1695, CVE-2013-1694, CVE-2013-1693, CVE-2013-1692, CVE-2013-1690, CVE-2013-1688, CVE-2013-1687, CVE-2013-1686, CVE-2013-1685, CVE-2013-1684, CVE-2013-1683, CVE-2013-1682 |
| Vendor Reference: | mfsa2013-49.html, mfsa2013-50.html, mfsa2013-51.html, mfsa2013-52.html, mfsa2013-53.html, mfsa2013-54.html, mfsa2013-55.html, mfsa2013-56.html, mfsa2013-57.html, mfsa2013-58.html, mfsa2013-59.html, mfsa2013-60.html, mfsa2013-61.html, mfsa2013-62.html |
| Bugtraq ID: | 60766,60773,60777,60778,60783,60787,60776,60784 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird:
1. Multiple memory corruption vulnerabilities exist in the browser engine that could lead to arbitrary code execution. [CVE-2013-1682, CVE-2013-1683]
2. Multiple use-after-free vulnerabilities exist in the 'mozilla::dom::HTMLMediaElement::LookupMediaElementURITable()', 'nsIDocument::GetRootElement()', and 'mozilla::ResetDir()' functions. [CVE-2013-1684, CVE-2013-1685, CVE-2013-1686]
3. A security vulnerability that may allow an attacker to run arbitrary code through XBL. This issue can be exploited to bypass Chrome Object Wrappers (COW) that may lead to cross-site scripting. [CVE-2013-1687]
4. An arbitrary code-execution that exists within Profiler. [CVE-2013-1688]
5. A denial-of-service vulnerability occurs when executing unmapped memory through the 'onreadystatechange' event. [CVE-2013-1690]
6. A cross-site request forgery vulnerability exists because data sent in the body of XMLHttpRequest (XHR) HEAD requests does not follow the XHR specification. [CVE-2013-1692]
7. An information-disclosure vulnerability exists due to the timing differences in the processing of SVG format images with filter. [CVE-2013-1693]
8. A denial-of-service vulnerability occurs when using 'PreserveWrapper' in cases where a wrapper is not set. [CVE-2013-1694]
9. A security-bypass vulnerability exists because the '<iframe sandbox>' restrictions are not applied to a frame element contained within a sandboxed iframe. [CVE-2013-1695]
10. A click-jacking issue exists because the X-Frame-Options header is ignored when a server push is used in multi-part responses. [CVE-2013-1696]
11. A security-bypass vulnerability occurs because 'XrayWrappers' can be bypassed to call the content-defined 'toString' and 'valueOf' methods through 'DefaultValue'. [CVE-2013-1697]
12. A security vulnerability exists because the 'getUserMedia' permission dialog incorrectly displays locations. [CVE-2013-1698]
13. A security vulnerability exists because of the incomplete Homograph attack prevention.[CVE-2013-1699]
14. A local privilege-escalation vulnerability exists because the Maintenance Service behaves incorrectly when the Mozilla Updater executable is inaccessible. [CVE-2013-1700]
Affected Versions:
Firefox prior to 22.0
Firefox ESR prior to 17.0.7
Thunderbird prior to 17.0.7
Thunderbird ESR  prior to 17.0.7

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to mfsa2013-49 (http://www.mozilla.org/security/announce/2013/mfsa2013-49.html), mfsa2013-50 (http://www.mozilla.org/security/announce/2013/mfsa2013-50.html), mfsa2013-51 (http://www.mozilla.org/security/announce/2013/mfsa2013-51.html), mfsa2013-52 (http://www.mozilla.org/security/announce/2013/mfsa2013-52.html), mfsa2013-53 (http://www.mozilla.org/security/announce/2013/mfsa2013-53.html), mfsa2013-54 (http://www.mozilla.org/security/announce/2013/mfsa2013-54.html), mfsa2013-55 (http://www.mozilla.org/security/announce/2013/mfsa2013-55.html), mfsa2013-56 (http://www.mozilla.org/security/announce/2013/mfsa2013-56.html), mfsa2013-57 (http://www.mozilla.org/security/announce/2013/mfsa2013-57.html),mfsa2013-58 (http://www.mozilla.org/security/announce/2013/mfsa2013-58.html), mfsa2013-59 (http://www.mozilla.org/security/announce/2013/mfsa2013-59.html), mfsa2013-60 (http://www.mozilla.org/security/announce/2013/mfsa2013-60.html),mfsa2013-61 (http://www.mozilla.org/security/announce/2013/mfsa2013-61.html), mfsa2013-62 (http://www.mozilla.org/security/announce/2013/mfsa2013-62.html) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 22.0: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/22.0/win32/en-US/Firefox%20Setup%2022.0.exe)
Firefox 22.0: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/22.0/mac/en-US/Firefox%2022.0.dmg)
Firefox ESR 17.0.7: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.7esr/win32/en-US/Firefox%20Setup%2017.0.7esr.exe)
Firefox ESR 17.0.7: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.7esr/mac/en-US/Firefox%2017.0.7esr.dmg)
Thunderbird 17.0.7: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.7/win32/en-US/Thunderbird%20Setup%2017.0.7.exe)
Thunderbird 17.0.7: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.7/mac/en-US/Thunderbird%2017.0.7.dmg)
Thunderbird ESR 17.0.7: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.7esr/mac/en-US/Thunderbird%2017.0.7esr.dmg)
Thunderbird ESR 17.0.7: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.7esr/win32/en-US/Thunderbird%20Setup%2017.0.7esr.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2013-1690

Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free - Metasploit Ref : /modules/exploit/windows/browser/mozilla_firefox_onreadystatechange

Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_firefox_onreadystatechange.

The Exploit-DB
Reference: CVE-2013-1690
Description: Mozilla Firefox - onreadystatechange Event DocumentViewerImpl Use-After-Free (Metasploit) - The Exploit-DB Ref : 27429
Link: http://www.exploit-db.com/exploits/27429

exploitdb
Reference: CVE-2013-1690
Description: Mozilla Firefox - onreadystatechange Event DocumentViewerImpl Use-After-Free (Metasploit)
Link: https://www.exploit-db.com/exploits/27429

seebug
Reference: CVE-2013-1690
Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free
Link: https://www.seebug.org/vuldb/ssvid-81039

saint
Reference: CVE-2013-1690
Description: Mozilla Firefox onreadystatechange Event Use After Free
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_onreadystatechange_use_after_free

packetstorm
Reference: CVE-2013-1690
Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free
Link: https://packetstormsecurity.com/files/122750/Firefox-onreadystatechange-Event-DocumentViewerImpl-Use-After-Free.html

metasploit
Reference: CVE-2013-1690
Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2013-1690
Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/mozilla_firefox_onreadysta

0day.today
Reference: CVE-2013-1690
Description: Firefox onreadystatechange Event DocumentViewerImpl Use After Free
Link: https://0day.today/exploit/21082

contagio
Reference: CVE-2013-1690
Description: LightsOut Exploit Kit
Link: https://docs.google.com/spreadsheets/d/1cK7vFVn73NTsoLU487nh-XVSFu7M064RgHeDZB0a2s8/edit#gid=0

cisa-kev
Reference: CVE-2013-1690
Description: Mozilla Firefox and Thunderbird Denial-of-Service Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: MetaSploit
Type: Hacktool
Platform: Script

Malware ID: Gif

Type: Trojan
Platform: Script

Malware ID: Heuristic
Type: Exploit
Platform: Script

Malware ID: CVE-2013-1690
Type: Exploit
Platform: Document,Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities

| | |
|---|---|
| QID: | 121374 |
| Category: | Local |
| Associated CVEs: | CVE-2013-1701, CVE-2013-1702, CVE-2013-1704, CVE-2013-1705, CVE-2013-1706, CVE-2013-1707, CVE-2013-1709, CVE-2013-1710, CVE-2013-1711, CVE-2013-1713, CVE-2013-1714, CVE-2013-1717, CVE-2013-1712, CVE-2013-1715, CVE-2013-1708 |
| Vendor Reference: | Mozilla, ,Mozilla |
| Bugtraq ID: | 61874,61867,61900,61876,61882,61896 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Multiple vulnerabilities have been reported in Mozilla products, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to conduct spoofing attacks, disclose potentially sensitive information, bypass certain security restrictions and compromise a user's system.
Affected Version:
All Mozilla Firefox versions prior to version 23.0
All Mozilla Firefox ESR version prior to 17.0.8
All Mozilla Thunderbird version prior to 17.0.8
All Mozilla Thunderbird ESR version prior to 17.0.8
All Mozilla SeaMonkey versions prior to 2.20

IMPACT:

Successful exploitation of the vulnerabilities allows the attacker to compromise the security of the user systems and gain control.

SOLUTION:

Users are recommended to update to latest version of the software. The latest version can be obtained here (https://www.mozilla.org/en-US/firefox/new/?icn=tabz)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox: Windows (https://www.mozilla.org/en-US/firefox/new/?icn=tabz)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2013-1710
Description: Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution - Metasploit Ref : /modules/exploit/multi/browser/firefox_proto_crmfrequest
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_proto_crmfrequest.rb

Reference: CVE-2013-1710
Description: Firefox toString console.time Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_tostring_console_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_tostring_console_injection.rb

The Exploit-DB
Reference: CVE-2013-1710
Description: Mozilla Firefox 5.0 < 15.0.1 - __exposedProps__ XCS Code Execution (Metasploit) - The Exploit-DB Ref : 30474
Link: http://www.exploit-db.com/exploits/30474

ExploitKits
Reference: CVE-2013-1710
Description: Niteris / CottonCastle
Link: http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

exploitdb
Reference: CVE-2013-1710
Description: Mozilla Firefox 5.0 < 15.0.1 - __exposedProps__ XCS Code Execution (Metasploit)
Link: https://www.exploit-db.com/exploits/30474

Reference: CVE-2013-1710
Description: Firefox toString console.time Privileged Javascript Injection
Link: https://www.exploit-db.com/exploits/34363

Reference: CVE-2013-1710
Description: Firefox 5.0 < 15.0.1 - __exposedProps__ XCS Code Execution (Metasploit)
Link: https://www.exploit-db.com/exploits/41682

seebug
Reference: CVE-2013-1710
Description: Firefox 5.0 - 15.0.1 - __exposedProps__ XCS Code Execution
Link: https://www.seebug.org/vuldb/ssvid-83857

saint
Reference: CVE-2013-1710
Description: Firefox crypto.generateCRMFRequest command execution
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_crypto_generatecrmfrequest

packetstorm
Reference: CVE-2013-1710
Description: Firefox toString console.time Privileged Javascript Injection
Link: https://packetstormsecurity.com/files/127915/Firefox-toString-console.time-Privileged-Javascript-Injection.html

Reference: CVE-2013-1710
Description: Firefox 15.0.1 Code Execution
Link: https://packetstormsecurity.com/files/124564/Firefox-15.0.1-Code-Execution.html

metasploit
Reference: CVE-2013-1710
Description: Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2013-1710
Description: Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_proto_crmfrequest.rb

Reference: CVE-2013-1710
Description: Firefox toString console.time Privileged Javascript Injection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_tostring_console_inject

0day.today

Reference: CVE-2013-1710
Description: Firefox toString console.time Privileged Javascript Injection Exploit
Link: https://0day.today/exploit/22528

Reference: CVE-2013-1710
Description: Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution Vulnerability
Link: https://0day.today/exploit/21704

contagio

Reference: CVE-2013-1710
Description: Niteris Exploit Kit
Link: https://docs.google.com/spreadsheets/d/1cK7vFVn73NTsoLU487nh-XVSFu7M064RgHeDZB0a2s8/edit#gid=0

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2013-1710
Type: Exploit
Platform: Script

Malware ID: CVE-2016-9079
Type: Exploit
Platform: Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-116 and MFSA 2015-133)

| | |
|---|---|
| QID: | 124192 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4513, CVE-2015-4514, CVE-2015-4515, CVE-2015-4518, CVE-2015-7185, CVE-2015-7186, CVE-2015-7187, CVE-2015-7188, CVE-2015-7189, CVE-2015-7190, CVE-2015-7191, CVE-2015-7192, CVE-2015-7193, CVE-2015-7194, CVE-2015-7195, CVE-2015-7196, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200, CVE-2015-7197, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-116 to MFSA 2015-133 |
| Bugtraq ID: | 91787,77411,77416,77415 |
| Service Modified: | 11/06/2015 |
| 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.
The Mozilla Foundation
has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 42
Mozilla
Firefox ESR versions prior to 38.4

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, obtain sensitive information, conduct spoofing attacks, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:

Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-85 to MFSA 2016-86)

| | |
|---|---|
| QID: | 370141 |
| Category: | Local |
| Associated CVEs: | CVE-2016-2827, CVE-2016-5256, CVE-2016-5257, CVE-2016-5270, CVE-2016-5271, CVE-2016-5272, CVE-2016-5273, CVE-2016-5274, CVE-2016-5275, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5279, CVE-2016-5280, CVE-2016-5281, CVE-2016-5282, CVE-2016-5283, CVE-2016-5284 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-85 to MFSA 2016-86 |
| Bugtraq ID: | 93049,93052 |
| Service Modified: | 03/07/2017 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.

A heap overflow may occur in nsCaseTransformTextRunFactory::TransformString() [CVE-2016-5270].

An invalid cast may occur in nsImageGeometryMixin() [CVE-2016-5272].

A use-after-free memory error may occur in mozilla::a11y::DocAccessible::ProcessInvalidationList() [CVE-2016-5276].

A use-after-free memory error may occur in nsFrameManager::CaptureFrameState() [CVE-2016-5274].

A use-after-free memory error may occur in nsRefreshDriver::Tick() [CVE-2016-5277].

A buffer overflow may occur in mozilla::gfx::FilterSupport::ComputeSourceNeededRegions() [CVE-2016-5275].

A buffer overflow may occur in nsBMPEncoder::AddImageFrame() [CVE-2016-5278].

A use-after-free memory error may occur in mozilla::nsTextNodeDirectionalityMap::RemoveElementFromMap() [CVE-2016-5280].

A use-after-free memory error may occur in DOMSVGLength() [CVE-2016-5281].

Various other errors may occur [CVE-2016-5256, CVE-2016-5257].

An out-of-bounds memory read error may occur in mozilla::net::IsValidReferrerPolicy() [CVE-2016-2827].

An error may occur in mozilla::a11y::HyperTextAccessible::GetChildOffset() [CVE-2016-5273].

An out-of-bounds read error may occur in PropertyProvider::GetSpacingInternal() [CVE-2016-5271].

A full path disclosure may occur after a drag and drop operation [CVE-2016-5279].

A favicon can be loaded via non-whiletlisted protocols [CVE-2016-5282].

A cross-origin 'iframe src' tag fragment timing attack may disclose data [CVE-2016-5283].
Affected Versions:
Mozilla Firefox versions prior to 49
Mozilla Firefox ESR versions prior to 45.4

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote
user can cause the target application to crash.

A remote user can obtain potentially sensitive information on the target system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory MFSA 2016-85 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-85/), MFSA 2016-86 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-86/) and Mozilla Security Advisories Page (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2016-85 to MFSA 2016-86 (https://www.mozilla.org/en-US/security/advisories/)
MFSA 2016-85 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-85/)
MFSA 2016-86 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-86/)

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 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2016-89,MFSA2016-90)

| | |
|---|---|
| QID: | 370225 |
| Category: | Local |
| Associated CVEs: | CVE-2016-5289, CVE-2016-5290, CVE-2016-5291, CVE-2016-5292, CVE-2016-5293, CVE-2016-5294, CVE-2016-5295, CVE-2016-5296, CVE-2016-5297, CVE-2016-5298, CVE-2016-5299, CVE-2016-9061, CVE-2016-9062, CVE-2016-9063, CVE-2016-9064, CVE-2016-9065, CVE-2016-9066, CVE-2016-9067, CVE-2016-9068, CVE-2016-9069, CVE-2016-9070, CVE-2016-9071, CVE-2016-9072, CVE-2016-9073, CVE-2016-9074, CVE-2016-9075, CVE-2016-9076, CVE-2016-9077 |
| Vendor Reference: | Mozilla Advisory 2016-89 |
| Bugtraq ID: | 94337,94335,94336,94339,94342,94341 |
| Service Modified: | 05/29/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.

A heap overflow may occur in Cairo in the processing of SVG content [CVE-2016-5296].
A URL parsing error may occur [CVE-2016-5292].
An argument length checking error may occur in JavaScript [CVE-2016-5297].
A buffer overflow may occur in nsScriptLoadHandler() [CVE-2016-9066].
A use-after-free memory error may occur in nsINode::ReplaceOrInsertBefore() [CVE-2016-9067].
A use-after-free memory error may occur in nsRefreshDriver() during web animations [CVE-2016-9068].
An integer overflow may occur in XML_Parse in the Expat library [CVE-2016-9063].
Other memory errors may occur [CVE-2016-5289, CVE-2016-5290].
A remote user can conduct a man-in-the-middle attack between the target user and the add-on update server to bypass certificate pinning protection and supply a specially crafted signed add-on [CVE-2016-9064].
On 64-bit Windows-based systems, the sandbox for 64-bin NPAPI plugins is not enabled by default when a new Firefox profile is created [CVE-2016-9072].
An extension can invoke the mozAddonManager API to gain elevated privileges [CVE-2016-9075].
A remote user can invoke a Canvas filter to conduct cross-origin timing attacks when images are loaded from third party locations [CVE-2016-9077].
A local user can bypass same-origin policy via local shortcut files to load arbitrary local content from disk [CVE-2016-5291].
A remote user can cause the Mozilla Maintenance Service to invoke the Mozilla Updater and run local files to potentially gain elevated privileges

[CVE-2016-5295]. Windows-based systems are affected.
A remote user can cause the SSL indicator to not be properly reset when loading a new page [CVE-2016-5298]. Android-based systems are affected.
On Android-based systems, an application on the system can intercept AuthTokens for applications with same signature-level permissions as Firefox [CVE-2016-5299].
On Android-based systems, an application on the system that defines a specific signature-level permissions used by Firefox can access Firefox API keys [CVE-2016-9061].
The browser retains some site metadata in 'browser.db' and 'browser.db-wal' after exiting private browsing mode [CVE-2016-9062]. Android-based systems are affected.
A web site loaded to the sidebar via a bookmark can reference a privileged chrome window and execute certain JavaScript operations to bypass cross-origin protections [CVE-2016-9070].
An extension can exploit a flaw in the windows.create schema and bypass security checks to load privileged URLs and potentially escape the WebExtension sandbox [CVE-2016-9073].
A user can exploit a weak mitigation in Network Security Services (NSS) for timing side-channel attacks with unspecified impact [CVE-2016-9074].
A remote user can exploit a flaw in the processing of Content Security Policy when redirecting from HTTP to HTTPS to determine if a specified web site is within the target user's browser history [CVE-2016-9071].
A local user can hardlink the Mozilla Updater log file in the working directory to another file on the target system to append data to the target file [CVE-2016-5293]. Windows-based systems are affected.
A local user can specify an arbitrary target working directory for the Mozilla Updater to write files to that directory [CVE-2016-5294]. Windows-based systems are affected.
A remote user can spoof the location bar via fullscreen mode [CVE-2016-9065]. Android-based systems are affected.
A remote user can use a 'select' drop down menu to spoof location bar content [CVE-2016-9076]. Systems with e10s enabled are affected.
Affected Versions :
Firefox  prior to 50.0
Firefox ESR prior to 45.5

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A local user
can obtain data on the target system.

A local user can modify files on the target system.

A remote user can bypass security controls on
the target system.

A remote user can obtain potentially sensitive information on the target system.

A remote user can spoof a URL.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2016-89: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2016-89/)
MFSA 2016-89: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2016-89/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2016-9061
Description: A previously installed malicious Android application which defines a specific signature-level permissions used by Firefox can access API keys meant for Firefox only. Note: This issue only affects Firefox for Android. Other versions and operating systems are unaffected. This vulnerability affects Firefox < 50.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1245795

Reference: CVE-2016-9062
Description: Private browsing mode leaves metadata information, such as URLs, for sites visited in "browser.db" and "browser.db-wal" files within the Firefox profile after the mode is exited. Note: This issue only affects Firefox for Android. Other versions and operating systems are unaffected. This vulnerability affects Firefox < 50.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1294438

Reference: CVE-2016-9065
Description: The location bar in Firefox for Android can be spoofed by forcing a user into fullscreen mode, blocking its exiting, and creating of a fake location bar without any user notification. Note: This issue only affects Firefox for Android. Other versions and operating systems are unaffected. This vulnerability affects Firefox < 50.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1306696

Reference: CVE-2016-5291
Description: A same-origin policy bypass with local shortcut files to load arbitrary local content from disk. This vulnerability affects

Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1292159

Reference: CVE-2016-5294

Description: The Mozilla Updater can be made to choose an arbitrary target working directory for output files resulting from the update process. This vulnerability requires local system access. Note: this issue only affects Windows operating systems. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1246972

Reference: CVE-2016-5298

Description: A mechanism where disruption of the loading of a new web page can cause the previous page's favicon and SSL indicator to not be reset when the new page is loaded. Note: this issue only affects Firefox for Android. Desktop Firefox is unaffected. This vulnerability affects Firefox < 50.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1227538

Reference: CVE-2016-5299

Description: A previously installed malicious Android application with same signature-level permissions as Firefox can intercept AuthTokens meant for Firefox only. Note: This issue only affects Firefox for Android. Other versions and operating systems are unaffected. This vulnerability affects Firefox < 50.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1245791

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox and Thunderbird SVG Animation Remote Code Execution Vulnerability (MFSA2016-92)

| | |
|---|---|
| QID: | 370245 |
| Category: | Local |
| Associated CVEs: | CVE-2016-9079 |
| Vendor Reference: | Mozilla Advisory 2016-92 |
| Bugtraq ID: | 94591 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a free and open-source web browser developed for Windows, OS X, and Linux.
Thunderbird is a free and open-source cross-platform email client developed for Windows, OS X, and Linux, with a mobile version for Android.
A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows.
Affected Versions :
Firefox prior to 50.0.2
Firefox prior to ESR 45.5.1
Thunderbird prior to 45.5.1

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2016-92 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2016-9079
Description: Firefox SVG Animation Remote Code Execution Exploit - Core Security Category : Exploits/Client Side

Metasploit
Reference: CVE-2016-9079
Description: Firefox nsSMILTimeContainer::NotifyTimeChange() RCE - Metasploit Ref : /modules/exploit/windows/browser/firefox_smil_uaf
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/firefox_smil_uaf.rb

The Exploit-DB
Reference: CVE-2016-9079
Description: Mozilla Firefox < 50.0.2 - 'nsSMILTimeContainer::NotifyTimeChange()' Remote Code Execution (Metasploit) - The Exploit-DB Ref : 41151
Link: http://www.exploit-db.com/exploits/41151

Reference: CVE-2016-9079
Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 42327
Link: http://www.exploit-db.com/exploits/42327

Qualys
Reference: CVE-2016-9079
Description: An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows.
Link: https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

exploitdb
Reference: CVE-2016-9079
Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/42327

Reference: CVE-2016-9079
Description: Mozilla Firefox < 50.0.2 - 'nsSMILTimeContainer::NotifyTimeChange()' Remote Code Execution (Metasploit)
Link: https://www.exploit-db.com/exploits/41151

nvd
Reference: CVE-2016-9079
Description: A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.
Link: https://www.exploit-db.com/exploits/41151/

Reference: CVE-2016-9079
Description: A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1321066

Reference: CVE-2016-9079
Description: A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.
Link: https://www.exploit-db.com/exploits/42327/

seebug
Reference: CVE-2016-9079
Description: New Firefox/Tor Browser 0-day vulnerability （CVE-2016-9079）
Link: https://www.seebug.org/vuldb/ssvid-92560

packetstorm
Reference: CVE-2016-9079
Description: Firefox nsSMILTimeContainer::NotifyTimeChange() Remote Code Execution
Link: https://packetstormsecurity.com/files/140696/Firefox-nsSMILTimeContainer-NotifyTimeChange-Remote-Code-Execution.html

Reference: CVE-2016-9079
Description: Firefox 50.0.1 ASM.JS JIT-Spray Remote Code Execution
Link: https://packetstormsecurity.com/files/143373/Firefox-50.0.1-ASM.JS-JIT-Spray-Remote-Code-Execution.html

metasploit
Reference: CVE-2016-9079
Description: Firefox nsSMILTimeContainer::NotifyTimeChange() RCE
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2016-9079
Description: Firefox nsSMILTimeContainer::NotifyTimeChange() RCE
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/firefox_smil_uaf.rb

cisa-alerts
Reference: CVE-2016-9079
Description: CISA Adds Six Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/06/22/cisa-adds-six-known-exploited-vulnerabilities-catalog

0day.today
Reference: CVE-2016-9079
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution Exploit
Link: https://0day.today/exploit/30001

Reference: CVE-2016-9079
Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution Exploit
Link: https://0day.today/exploit/30002

Reference: CVE-2016-9079
Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution Exploit
Link: https://0day.today/exploit/28138

Reference: CVE-2016-9079
Description: Mozilla Firefox nsSMILTimeContainer::NotifyTimeChange() Remote Code Execution Exploit
Link: https://0day.today/exploit/26792

coreimpact
Reference: CVE-2016-9079
Description: Firefox SVG Animation Remote Code Execution Exploit
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev
Reference: CVE-2016-9079
Description: Mozilla Firefox, Firefox ESR, and Thunderbird Use-After-Free Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2016-9079
Description: Mozilla Firefox Use-after-free in SVG Animation (Tor exploit)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2019-8039
Type: Exploit
Platform: Document

Malware ID: CVE-2016-9079
Type: Exploit
Platform: Win32,Binary,Text,Script

| | |
|---|---|
| Malware ID: | ISqrlFX |
| Type: | Exploit |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | Pdfka |
| Type: | Exploit |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | CVE-2004-0636 |
| Type: | Exploit |
| Platform: | Document |

| | |
|---|---|
| Malware ID: | CVE-2019-8038 |
| Type: | Exploit |
| Platform: | Document |

| | |
|---|---|
| Malware ID: | Heuristic |
| Type: | Exploit |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | ShellCode |
| Type: | Trojan |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | WebShell |
| Type: | Trojan |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | Cryxos |
| Type: | Trojan |
| Platform: | Script |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2016-94,MFSA2016-95)

| | |
|---|---|
| QID: | 370264 |
| Category: | Local |
| Associated CVEs: | CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904, CVE-2016-9905 |
| Vendor Reference: | MFSA 2016-94 to 2016-95 |
| Bugtraq ID: | 94883,94885 |
| Service Modified: | 08/02/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.
A remote user can create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A buffer overflow may occur in SkiaGl caused when a GrGLBuffer is truncated during allocation [CVE-2016-9894]. Mozilla ESR is not affected.

A use-after-free memory error may occur when manipulating DOM events and removing audio elements [CVE-2016-9899].

A use-after-free may occur in WebVR [CVE-2016-9896]. Mozilla ESR is not affected.

A memory corruption error may occur in libGLES [CVE-2016-9897].

A use-after-free memory may occur when manipulating DOM subtrees in the Editor [CVE-2016-9898].

Other code execution errors may occur [CVE-2016-9080, CVE-2016-9893]. Mozilla ESR is not affected by CVE-2016-9080.

A remote user can bypass inline JavaScript Content Security Policy (CSP) and cause event handlers on marquee elements to be executed [CVE-2016-9895].

A remote user can create a specially crafted SVG image that, when loaded by the target user, will access restricted external resources via 'data:' URLs [CVE-2016-9900].

A remote user can conduct a JavaScript Map/Set timing attack to obtain potentially sensitive information (e.g., usernames embedded in JavaScript code) from other domains [CVE-2016-9904].

A remote user can exploit an input validation flaw in the Pocket server to execute arbitrary JavaScript in the about:pocket-saved page and access the Pocket messaging API [CVE-2016-9901].

A remote user can exploit an origin validation flaw in the Pocket toolbar to inject content and commands into the Pocket context [CVE-2016-9902]. Systems with e10s enabled are not affected.
Affected Versions
Firefox  prior to 50.1
Firefox ESR prior to 45.6

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote user
can bypass security controls on the target system.

A remote user can obtain potentially sensitive information on the target system.

A remote
user can access the target user's cookies (including authentication cookies), if any, associated with an arbitrary site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to MFSA 2016-94 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/), MFSA 2016-95 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-95/) and Mozilla Security Advisories Page (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2016-94: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/)
mfsa2016-94: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/)
mfsa2016-95: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2016-95/)
mfsa2016-95: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2016-95/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security
Reference: CVE-2016-9899
Description: Mozilla Firefox Use After Free DOM and Audio Elements Exploit - Core Security Category : Exploits/Client Side

The Exploit-DB
Reference: CVE-2016-9899
Description: Mozilla Firefox < 50.1.0 - Use-After-Free - The Exploit-DB Ref : 41042
Link: http://www.exploit-db.com/exploits/41042

exploitdb
Reference: CVE-2016-9899
Description: Mozilla Firefox < 50.1.0 - Use-After-Free
Link: https://www.exploit-db.com/exploits/41042

nvd
Reference: CVE-2016-9895

Description: Event handlers on "marquee" elements were executed despite a strict Content Security Policy (CSP) that disallowed inline JavaScript. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1312272

Reference: CVE-2016-9896

Description: Use-after-free while manipulating the "navigator" object within WebVR. Note: WebVR is not currently enabled by default. This vulnerability affects Firefox < 50.1.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1315543

Reference: CVE-2016-9897

Description: Memory corruption resulting in a potentially exploitable crash during WebGL functions using a vector constructor with a varying array within libGLES. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1301381

Reference: CVE-2016-9898

Description: Use-after-free resulting in potentially exploitable crash when manipulating DOM subtrees in the Editor. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1314442

Reference: CVE-2016-9899

Description: Use-after-free while manipulating DOM events and removing audio elements due to errors in the handling of node adoption. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1317409

Reference: CVE-2016-9900

Description: External resources that should be blocked when loaded by SVG images can bypass security restrictions through the use of "data:" URLs. This could allow for cross-domain data leakage. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1319122

Reference: CVE-2016-9902

Description: The Pocket toolbar button, once activated, listens for events fired from it's own pages but does not verify the origin of incoming events. This allows content from other origins to fire events and inject content and commands into the Pocket context. Note: this issue does not affect users with e10s enabled. This vulnerability affects Firefox ESR < 45.6 and Firefox < 50.1.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1320039

Reference: CVE-2016-9905

Description: A potentially exploitable crash in "EnumerateSubDocuments" while adding or removing sub-documents. This vulnerability affects Firefox ESR < 45.6 and Thunderbird < 45.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1293985

seebug

Reference: CVE-2016-9899

Description: Mozilla Firefox Use-After-Free（CVE-2016-9899）

Link: https://www.seebug.org/vuldb/ssvid-92622

packetstorm

Reference: CVE-2016-9899

Description: Mozilla Firefox Use-After-Free

Link: https://packetstormsecurity.com/files/140491/Mozilla-Firefox-Use-After-Free.html

0day.today

Reference: CVE-2016-9899

Description: Mozilla Firefox 50.1.0 - Use After Free Exploit

Link: https://0day.today/exploit/26670

coreimpact

Reference: CVE-2016-9899

Description: Mozilla Firefox Use-after-free DOM and Audio Elements Exploit

Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2017-01,MFSA2017-02)

| | |
|---|---|
| QID: | 370289 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5373, CVE-2017-5374, CVE-2017-5375, CVE-2017-5376, CVE-2017-5377, CVE-2017-5378, CVE-2017-5379, CVE-2017-5380, CVE-2017-5381, CVE-2017-5382, CVE-2017-5383, CVE-2017-5384, CVE-2017-5385, CVE-2017-5386, CVE-2017-5387, CVE-2017-5388, CVE-2017-5389, CVE-2017-5390, CVE-2017-5391, CVE-2017-5392, CVE-2017-5393, CVE-2017-5394, CVE-2017-5395, CVE-2017-5396 |
| Vendor Reference: | MFSA 2017-01 to 2017-02 |
| Bugtraq ID: | 95761,95769,95763,95762,95759,95757,95758 |
| Service Modified: | 05/29/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.
CVE-2017-5375: Excessive JIT code allocation allows bypass of ASLR and DEP
CVE-2017-5376: Use-after-free in XSL
CVE-2017-5377: Memory corruption with transforms to create gradients in Skia
CVE-2017-5378: Pointer and frame data leakage of Javascript objects
CVE-2017-5379: Use-after-free in Web Animations
CVE-2017-5380: Potential use-after-free during DOM manipulations
CVE-2017-5390: Insecure communication methods in Developer Tools JSON viewer
CVE-2017-5389: WebExtensions can install additional add-ons via modified host requests
CVE-2017-5396: Use-after-free with Media Decoder
CVE-2017-5381: Certificate Viewer exporting can be used to navigate and save to arbitrary filesystem locations
CVE-2017-5382: Feed preview can expose privileged content errors and exceptions
CVE-2017-5383: Location bar spoofing with unicode characters
CVE-2017-5384: Information disclosure via Proxy Auto-Config (PAC)
CVE-2017-5385: Data sent in multipart channels ignores referrer-policy response headers
CVE-2017-5386: WebExtensions can use data: protocol to affect other extensions
CVE-2017-5394: Android location bar spoofing using fullscreen and JavaScript events
CVE-2017-5391: Content about: pages can load privileged about: pages
CVE-2017-5392: Weak references using multiple threads on weak proxy objects lead to unsafe memory usage
CVE-2017-5393: Remove addons.mozilla.org CDN from whitelist for mozAddonManager
CVE-2017-5395: Android location bar spoofing during scrolling
CVE-2017-5387: Disclosure of local file existence through TRACK tag error messages
CVE-2017-5388: WebRTC can be used to generate a large amount of UDP traffic for DDOS attacks
CVE-2017-5374: Memory safety bugs fixed in Firefox 51
CVE-2017-5373: Memory safety bugs fixed in Firefox 51 and Firefox ESR 45.7
Affected Versions
Firefox  prior to 51
Firefox ESR prior to 45.7

IMPACT:

A use-after-free memory error may occur in XSL when processing XSLT documents [CVE-2017-5376].

A memory corruption error may occur in Skia
when using transforms to make gradients [CVE-2017-5377].

A use-after-free memory error may occur in Web Animations when interacting with
cycle collection [CVE-2017-5379].

A use-after-free memory error may occur in processing SVG content [CVE-2017-5380].

A use-after-free
memory error may occur in Media Decoder [CVE-2017-5396].

A remote user can exploit a proxy object thread reference flaw to potentially
execute arbitrary code [CVE-2017-5392]. Android systems are affected.

Various memory corruption errors may occur [CVE-2017-5373,

CVE-2017-5374].

A remote user can spoof URLs using certain unicode glyphs for alternative hyphens and quotes [CVE-2017-5383].

A remote
user can spoof URLs [CVE-2017-5394, CVE-2017-5395]. Android systems are affected.

A remote user can can exploit a JIT code allocation flaw
to bypass address space layout randomization (ASLR) and data execution prevention (DEP) security features [CVE-2017-5375].

A remote user can
determine an object's address via shared hash codes [[CVE-2017-5378].

A remote user that can monitor the network may be able to view
potentially sensitive information in JSON and HTTP headers sent to the target user's JSON viewer in Developer Tools [CVE-2017-5390].

A
remote user can cause the Certificate Viewer to save an exported certificate to arbitrary filesystem locations [CVE-2017-5381].

A remote
user can exploit a flaw in the feed preview feature for RSS feeds to view errors and exceptions generated by privileged content
[CVE-2017-5382].

A remote user can exploit a Proxy Auto-Config bug to obtain potentially sensitive information [CVE-2017-5384].

The
browser may ignore the referrer-policy response header in certain cases [CVE-2017-5385]. As a result, a remote user can obtain potentially
sensitive information.

A specially crafted WebExtension script can invoke the 'data:' protocol to access data from pages loaded by other web
extensions or gain elevated privileges [CVE-2017-5386].

A specially crafted 'about:' page can load privileged 'about:' pages to potentially
gain elevated privileges [CVE-2017-5391].

A specially crafted extension can invoke mozAddonManager to install additional extensions
[CVE-2017-5393].

A specially crafted CSP header can invoke the mozAddonManager API to install additional add-ons [CVE-2017-5389].

A
remote user can invoke TRACK tag errors to determine if a specified file exists on the target system [CVE-2017-5387].

A remote user can use
a STUN server in conjunction with a large number of webkitRTCPeerConnection objects to conduct denial of service attacks against other systems
[CVE-2017-5388]. e10s systems are affected.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to MFSA 2017-01
(https://www.mozilla.org/en-US/security/advisories/mfsa2017-01/), MFSA 2017-02 (https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/) and Mozilla
Security Advisories Page (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-01: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-01/)
mfsa2017-01: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-01/)
mfsa2017-02: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/)
mfsa2017-02: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


The Exploit-DB

Reference: CVE-2017-5375
Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 42327
Link: http://www.exploit-db.com/exploits/42327

Reference: CVE-2017-5375
Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 44293
Link: http://www.exploit-db.com/exploits/44293

Reference: CVE-2017-5375
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 44294
Link: http://www.exploit-db.com/exploits/44294

exploitdb

Reference: CVE-2017-5375
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/44294

Reference: CVE-2017-5375
Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/42327

Reference: CVE-2017-5375
Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/44293

nvd

Reference: CVE-2017-5374
Description: Memory safety bugs were reported in Firefox 50.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 51.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1325344%2C1317501%2C1311319%2C1329989%2C1300145%2C1322305%2C1288561%2C1295747%

Reference: CVE-2017-5375
Description: JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
Link: https://www.exploit-db.com/exploits/44294/

Reference: CVE-2017-5375
Description: JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
Link: https://www.exploit-db.com/exploits/42327/

Reference: CVE-2017-5375
Description: JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
Link: https://www.exploit-db.com/exploits/44293/

Reference: CVE-2017-5378
Description: Hashed codes of JavaScript objects are shared between pages. This allows for pointer leaks because an object's address can be discovered through hash codes, and also allows for data leakage of an object's content using these hash codes. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1312001

Reference: CVE-2017-5379
Description: Use-after-free vulnerability in Web Animations when interacting with cycle collection found through fuzzing. This vulnerability affects Firefox < 51.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1309198

Reference: CVE-2017-5384
Description: Proxy Auto-Config (PAC) files can specify a JavaScript function called for all URL requests with the full URL path which exposes more information than would be sent to the proxy itself in the case of HTTPS. Normally the Proxy Auto-Config file is specified by the user or machine owner and presumed to be non-malicious, but if a user has enabled Web Proxy Auto Detect (WPAD) this file can be served remotely. This vulnerability affects Firefox < 51.
Link: https://www.contextis.com//resources/blog/leaking-https-urls-20-year-old-vulnerability/

Reference: CVE-2017-5385
Description: Data sent with in multipart channels, such as the multipart/x-mixed-replace MIME type, will ignore the referrer-policy response header, leading to potential information disclosure for sites using this header. This vulnerability affects Firefox < 51.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1295945

Reference: CVE-2017-5386
Description: WebExtension scripts can use the "data:" protocol to affect pages loaded by other web extensions using this protocol, leading to potential data disclosure or privilege escalation in affected extensions. This vulnerability affects Firefox ESR < 45.7 and Firefox < 51.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1319070

Reference: CVE-2017-5387

Description: The existence of a specifically requested local file can be found due to the double firing of the "onerror" when the "source" attribute on a "" tag refers to a file that does not exist if the source page is loaded locally. This vulnerability affects Firefox < 51.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1295023

Reference: CVE-2017-5389

Description: WebExtensions could use the "mozAddonManager" API by modifying the CSP headers on sites with the appropriate permissions and then using host requests to redirect script loads to a malicious site. This allows a malicious extension to then install additional extensions without explicit user permission. This vulnerability affects Firefox < 51.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1308688

Reference: CVE-2017-5394

Description: A location bar spoofing attack where the location bar of loaded page will be shown over the content of another tab due to a series of JavaScript events combined with fullscreen mode. Note: This issue only affects Firefox for Android. Other operating systems are not affected. This vulnerability affects Firefox < 51.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1222798

Reference: CVE-2017-5395

Description: Malicious sites can display a spoofed location bar on a subsequently loaded page when the existing location bar on the new page is scrolled out of view if navigations between pages can be timed correctly. Note: This issue only affects Firefox for Android. Other operating systems are not affected. This vulnerability affects Firefox < 51.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1293463

Reference: CVE-2017-5396

Description: A use-after-free vulnerability in the Media Decoder when working with media files when some events are fired after the media elements are freed from memory. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1329403

packetstorm

Reference: CVE-2017-5375

Description: Firefox 50.0.1 ASM.JS JIT-Spray Remote Code Execution

Link: https://packetstormsecurity.com/files/143373/Firefox-50.0.1-ASM.JS-JIT-Spray-Remote-Code-Execution.html

Reference: CVE-2017-5375

Description: Firefox 46.0.1 ASM.JS JIT-Spray Remote Code Execution

Link: https://packetstormsecurity.com/files/146818/Firefox-46.0.1-ASM.JS-JIT-Spray-Remote-Code-Execution.html

Reference: CVE-2017-5375

Description: Firefox 44.0.2 ASM.JS JIT-Spray Remote Code Execution

Link: https://packetstormsecurity.com/files/146819/Firefox-44.0.2-ASM.JS-JIT-Spray-Remote-Code-Execution.html

0day.today

Reference: CVE-2017-5375

Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution Exploit

Link: https://0day.today/exploit/30001

Reference: CVE-2017-5375

Description: Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution Exploit

Link: https://0day.today/exploit/28138

Reference: CVE-2017-5375

Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution Exploit

Link: https://0day.today/exploit/30002

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2017-5375

Type: Exploit

Platform: Script

Malware ID: Heuristic

Type: Exploit

Platform: Script

| | |
|---|---|
| Malware ID: | CVE-2016-9079 |
| Type: | Exploit |
| Platform: | Script |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2017-05,MFSA2017-06)

| | |
|---|---|
| QID: | 370325 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410, CVE-2017-5411, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5425, CVE-2017-5426, CVE-2017-5427 |
| Vendor Reference: | MFSA 2017-05 to 2017-06 |
| Bugtraq ID: | 96692,96694,96677,96664,96691,96693,96651,96696,96654 |
| Service Modified: | 08/02/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.
A remote user can exploit a flaw in 'asm.js' to bypass ASLR and DEP security features on the target system [CVE-2017-5400].

A remote user can create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A memory corruption error may occur in handling ErrorResult [CVE-2017-5401].

A use-after-free memory error may occur in processing events in FontFace objects [CVE-2017-5402].

A use-after-free memory error may occur when using addRange [CVE-2017-5403].

A use-after-free memory error may occur when using ranges in selections [CVE-2017-5404].

A memory corruption error may occur during JavaScript garbage collection incremental sweeping [CVE-2017-5410].

A use-after-free memory error may occur in libGLES [CVE-2017-5411]. Windows-based systems are affected.

Other memory corruption errors may occur [CVE-2017-5398, CVE-2017-5399].

A remote user can delete files on the target system via a callback parameter in Mozilla Windows Updater and Maintenance Service [CVE-2017-5409]. Windows-based systems are affected.

A remote user can cause denial of service conditions.

A remote user can trigger a segmentation fault in Skia during some canvas operations [CVE-2017-5406].

A remote user can invoke the 'view-source:' protocol repeatedly in a single hyperlink to cause the browser to crash [CVE-2017-5422].

A remote user can trigger a segmentation fault during some bidirectional layout operations [CVE-2017-5413].

A remote user can trigger a null pointer dereference in HttpChannel to cause the browser to crash [CVE-2017-5416].

A remote server can repeatedly trigger a modal authentication prompt to cause the target connected user's browser to become non-responsive [CVE-2017-5419].

A remote user can conduct floating-point timing side channel attacks using SVG filters to access pixel values and obtain history and text information from other domains [CVE-2017-5407].

A remote user can load video captions from other domains [CVE-2017-5408].

A remote user can trigger a buffer read error in SVG filter color value operations to obtain potentially sensitive data [CVE-2017-5412].

A remote user can send specially crafted HTTP digest authorization responses to trigger an out-of-bounds memory read error and leak potentially sensitive information [CVE-2017-5418].

The file picker dialog may choose and display the wrong local default directory, allowing a remote user to obtain potentially sensitive information, such as the operating system or the local account name [CVE-2017-5414].

A remote user can spoof URLs via a 'blob:' protocol [CVE-2017-5415].

A remote user can spoof address bar data via drag and drop URLs [CVE-2017-5417].

A remote user can use a 'javascript:' url to obfuscate the addressbar location [CVE-2017-5420].

A remote user can spoof the contents of the print preview window [CVE-2017-5421].

A remote user can exploit overly permissive Gecko Media Plugin sandbox regular expression access controls to obtain data in subdirectories of '/private/var' [CVE-2017-5425]. OS X is affected.

A remote user can bypass Gecko Media Plugin sandbox restrictions when the seccomp-bpf filter is running [CVE-2017-5426]. Linux is affected.

A local user can create a specially crafted 'chrome.manifest' file to cause arbitrary software to added [CVE-2017-5427].

A remote user can supply specially crafted FTP response codes to cause the target connected user's browser to use of uninitialized values for ports in FTP operations [CVE-2017-5405].
Affected Versions
Firefox prior to 52, ESR prior to 45.8

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote
user can cause denial of service conditions.

A remote user can delete files on the target system.

A remote user can bypass security
controls on the target system.

A remote user can obtain potentially sensitive information on the target system.

A remote user can spoof
a URL.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to MFSA 2017-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/), MFSA 2017-06 (https://www.mozilla.org/en-US/security/advisories/mfsa2017-06/) and Mozilla Security Advisories Page (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-05: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/)
mfsa2017-06: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-06/)
mfsa2017-05: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/)
mfsa2017-06: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-06/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2017-5404
Description: Mozilla Firefox - 'table' Use-After-Free - The Exploit-DB Ref : 41660
Link: http://www.exploit-db.com/exploits/41660

Reference: CVE-2017-5415
Description: Mozilla Firefox - Address Bar Spoofing - The Exploit-DB Ref : 44266
Link: http://www.exploit-db.com/exploits/44266

exploitdb

Reference: CVE-2017-5415
Description: Mozilla Firefox - Address Bar Spoofing
Link: https://www.exploit-db.com/exploits/44266

Reference: CVE-2017-5404
Description:

Mozilla Firefox - 'table' Use-After-Free

Link: https://www.exploit-db.com/exploits/41660

nvd

Reference: CVE-2017-5401

Description: A crash triggerable by web content in which an "ErrorResult" references unassigned memory due to a logic error. The resulting crash may be exploitable. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1328861

Reference: CVE-2017-5404

Description: A use-after-free error can occur when manipulating ranges in selections with one node inside a native anonymous tree and one node outside of it. This results in a potentially exploitable crash. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1340138

Reference: CVE-2017-5404

Description: A use-after-free error can occur when manipulating ranges in selections with one node inside a native anonymous tree and one node outside of it. This results in a potentially exploitable crash. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://www.exploit-db.com/exploits/41660/

Reference: CVE-2017-5405

Description: Certain response codes in FTP connections can result in the use of uninitialized values for ports in FTP operations. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1336699

Reference: CVE-2017-5406

Description: A segmentation fault can occur in the Skia graphics library during some canvas operations due to issues with mask/clip intersection and empty masks. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1306890

Reference: CVE-2017-5407

Description: Using SVG filters that don't use the fixed point math implementation on a target iframe, a malicious page can extract pixel values from a targeted user. This can be used to extract history information and read text values across domains. This violates same-origin policy and leads to information disclosure. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1336622

Reference: CVE-2017-5408

Description: Video files loaded video captions cross-origin without checking for the presence of CORS headers permitting such cross-origin use, leading to potential information disclosure for video captions. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1313711

Reference: CVE-2017-5409

Description: The Mozilla Windows updater can be called by a non-privileged user to delete an arbitrary local file by passing a special path to the callback parameter through the Mozilla Maintenance Service, which has privileged access. Note: This attack requires local system access and only affects Windows. Other operating systems are not affected. This vulnerability affects Firefox ESR < 45.8 and Firefox < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1321814

Reference: CVE-2017-5410

Description: Memory corruption resulting in a potentially exploitable crash during garbage collection of JavaScript due errors in how incremental sweeping is managed for memory cleanup. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1330687

Reference: CVE-2017-5411

Description: A use-after-free can occur during buffer storage operations within the ANGLE graphics library, used for WebGL content. The buffer storage can be freed while still in use in some circumstances, leading to a potentially exploitable crash. Note: This issue is in "libGLES", which is only in use on Windows. Other operating systems are not affected. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1325511

Reference: CVE-2017-5413

Description: A segmentation fault can occur during some bidirectional layout operations. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1337504

Reference: CVE-2017-5415

Description: An attack can use a blob URL and script to spoof an arbitrary addressbar URL prefaced by "blob:" as the protocol, leading to user confusion and

further spoofing attacks. This vulnerability affects Firefox < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1321719

Reference: CVE-2017-5416

Description: In certain circumstances a networking event listener can be prematurely released. This appears to result in a null dereference in practice. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1328121

Reference: CVE-2017-5418

Description: An out of bounds read error occurs when parsing some HTTP digest authorization responses, resulting in information leakage through the reading of random memory containing matches to specifically set patterns. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1338876

Reference: CVE-2017-5419

Description: If a malicious site repeatedly triggers a modal authentication prompt, eventually the browser UI will become non-responsive, requiring shutdown through the operating system. This is a denial of service (DOS) attack. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1312243

Reference: CVE-2017-5420

Description: A "javascript:" url loaded by a malicious page can obfuscate its location by blanking the URL displayed in the addressbar, allowing for an attacker to spoof an existing page without the malicious page's address being displayed correctly. This vulnerability affects Firefox < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1284395

Reference: CVE-2017-5421

Description: A malicious site could spoof the contents of the print preview window if popup windows are enabled, resulting in user confusion of what site is currently loaded. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1301876

Reference: CVE-2017-5422

Description: If a malicious site uses the "view-source:" protocol in a series within a single hyperlink, it can trigger a non-exploitable browser crash when the hyperlink is selected. This was fixed by no longer making "view-source:" linkable. This vulnerability affects Firefox < 52 and Thunderbird < 52.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1295002

seebug

Reference: CVE-2017-5414

Description: Mozilla Firefox webkitdirectory local files disclosure (CVE-2017-5414)

Link: https://www.seebug.org/vuldb/ssvid-92955

Reference: CVE-2017-5404

Description: Mozilla Firefox table use-after-free（CVE-2017-5404）

Link: https://www.seebug.org/vuldb/ssvid-92853

0day.today

Reference: CVE-2017-5404

Description: Mozilla Firefox - table Use-After-Free Exploit

Link: https://0day.today/exploit/27356

Reference: CVE-2017-5415

Description: Mozilla Firefox - Address Bar Spoofing Exploit

Link: https://0day.today/exploit/29973

github-exploits

Reference: CVE-2017-5415

Description: 649/CVE-2017-5415 exploit repository

Link: https://github.com/649/CVE-2017-5415

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 5 Mozilla Firefox Integer Overflow Vulnerability (MFSA2017-08)

| | |
|---|---|
| QID: | 370341 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5428 |
| Vendor Reference: | mfsa2017-08 |
| Bugtraq ID: | 96959 |
| Service Modified: | 05/30/2023 |
| 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.
A remote user can create specially crafted content that, when loaded by the target user, will trigger an integer overflow in the createImageBitmap() function and execute arbitrary code on the target user's system. The code will run in the content sandbox.
Affected Version :
Firefox 52.0
Firefox ESR 52.0; possibly prior versions

IMPACT:

A remote user can create specially crafted content that, when loaded by the target user, will trigger an integer overflow in the createImageBitmap() function and execute arbitrary code on the target user's system.

SOLUTION:

The vendor has issued a fix (52.0.1, ESR 52.0.1). Refer to MFSA 2017-08 (https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/), Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-08: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/)
mfsa2017-08: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

| | |
|---|---|
| Reference: | CVE-2017-5428 |
| Description: | An integer overflow in "createImageBitmap()" was reported through the Pwn2Own contest. The fix for this vulnerability disables the experimental extensions to the "createImageBitmap" API. This function runs in the content sandbox, requiring a second vulnerability to compromise a user's computer. This vulnerability affects Firefox ESR < 52.0.1 and Firefox < 52.0.1. |
| Link: | https://bugzilla.mozilla.org/show_bug.cgi?id=1348168 |

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities. (MFSA2017-10 to MFSA2017-12)

| | |
|---|---|
| QID: | 370375 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5450, CVE-2017-5451, CVE-2017-5452, CVE-2017-5453, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5458, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5463, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469, CVE-2016-6354 |
| Vendor Reference: | mfsa2017-10 to mfsa2017-12 |
| Bugtraq ID: | 98050,97940,103053 |
| Service Modified: | 07/29/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can obtain files on the target system. A remote user can spoof URLs. A remote user can conduct cross-site scripting attacks.
A remote user can create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system.
Affected Version :
Firefox prior to 53.0
Firefox ESR prior to 52.1
Firefox ESR prior to 45.9

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote
user can obtain files on the target system.

A remote user can spoof a URL.

A remote user can access the target user's cookies
(including authentication cookies), if any, associated with an arbitrary site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

SOLUTION:

The vendor has issued a fix (53.0). Refer to MFSA 2017-10 to MFSA 2017-12 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-10 to mfsa2017-12: Windows (https://www.mozilla.org/en-US/security/advisories/)
mfsa2017-10 to mfsa2017-12: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2017-5447
Description: Mozilla Firefox < 53 - 'gfxTextRun' Out-of-Bounds Read - The Exploit-DB Ref : 42071
Link: http://www.exploit-db.com/exploits/42071

Reference: CVE-2017-5465
Description: Mozilla Firefox < 53 - 'ConvolvePixel' Memory Disclosure - The Exploit-DB Ref : 42072
Link: http://www.exploit-db.com/exploits/42072

exploitdb

Reference: CVE-2017-5465
Description: Mozilla Firefox < 53 - 'ConvolvePixel' Memory Disclosure
Link: https://www.exploit-db.com/exploits/42072

Reference: CVE-2017-5447
Description: Mozilla Firefox < 53 - 'gfxTextRun' Out-of-Bounds Read
Link: https://www.exploit-db.com/exploits/42071

nvd

Reference: CVE-2017-5443
Description: An out-of-bounds write vulnerability while decoding improperly formed BinHex format archives. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1342661

Reference: CVE-2017-5445
Description: A vulnerability while parsing "application/http-index-format" format content where uninitialized values are used to create an array. This could allow the reading of uninitialized memory into the arrays affected. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1344467

Reference: CVE-2017-5446

Description: An out-of-bounds read when an HTTP/2 connection to a servers sends "DATA" frames with incorrect data content. This leads to a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1343505

Reference: CVE-2017-5447

Description: An out-of-bounds read during the processing of glyph widths during text layout. This results in a potentially exploitable crash and could allow an attacker to read otherwise inaccessible memory. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1343552

Reference: CVE-2017-5447

Description: An out-of-bounds read during the processing of glyph widths during text layout. This results in a potentially exploitable crash and could allow an attacker to read otherwise inaccessible memory. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://www.exploit-db.com/exploits/42071/

Reference: CVE-2017-5450

Description: A mechanism to spoof the Firefox for Android addressbar using a "javascript:" URI. On Firefox for Android, the base domain is parsed incorrectly, making the resulting location less visibly a spoofed site and showing an incorrect domain in appended notifications. This vulnerability affects Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1325955

Reference: CVE-2017-5451

Description: A mechanism to spoof the addressbar through the user interaction on the addressbar and the "onblur" event. The event could be used by script to affect text display to make the loaded site appear to be different from the one actually loaded within the addressbar. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1273537

Reference: CVE-2017-5452

Description: Malicious sites can display a spoofed addressbar on a page when the existing location bar on the new page is scrolled out of view if an HTML editable page element is user selected. Note: This attack only affects Firefox for Android. Other operating systems are not affected. This vulnerability affects Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1344517

Reference: CVE-2017-5455

Description: The internal feed reader APIs that crossed the sandbox barrier allowed for a sandbox escape and escalation of privilege if combined with another vulnerability that resulted in remote code execution inside the sandboxed process. This vulnerability affects Firefox ESR < 52.1 and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1341191

Reference: CVE-2017-5456

Description: A mechanism to bypass file system access protections in the sandbox using the file system request constructor through an IPC message. This allows for read and write access to the local file system. This vulnerability affects Firefox ESR < 52.1 and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1344415

Reference: CVE-2017-5458

Description: When a "javascript:" URL is drag and dropped by a user into the addressbar, the URL will be processed and executed. This allows for users to be socially engineered to execute an XSS attack on themselves. This vulnerability affects Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1229426

Reference: CVE-2017-5459

Description: A buffer overflow in WebGL triggerable by web content, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1333858

Reference: CVE-2017-5460

Description: A use-after-free vulnerability in frame selection triggered by a combination of malicious script content and key presses by a user. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1343642

Reference: CVE-2017-5465

Description: An out-of-bounds read while processing SVG content in "ConvolvePixel". This results in a crash and also allows for otherwise inaccessible memory being copied into SVG graphic content, which could then displayed. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

Link: https://www.exploit-db.com/exploits/42072/

Reference: CVE-2017-5465
Description: An out-of-bounds read while processing SVG content in "ConvolvePixel". This results in a crash and also allows for otherwise inaccessible memory being copied into SVG graphic content, which could then displayed. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1347617

Reference: CVE-2017-5466
Description: If a page is loaded from an original site through a hyperlink and contains a redirect to a "data:text/html" URL, triggering a reload will run the reloaded "data:text/html" page with its origin set incorrectly. This allows for a cross-site scripting (XSS) attack. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1353975

Reference: CVE-2017-5433
Description: A use-after-free vulnerability in SMIL animation functions occurs when pointers to animation elements in an array are dropped from the animation controller while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1347168

Reference: CVE-2017-5434
Description: A use-after-free vulnerability occurs when redirecting focus handling which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1349946

Reference: CVE-2017-5438
Description: A use-after-free vulnerability during XSLT processing due to the result handler being held by a freed handler during handling. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1336828

Reference: CVE-2017-5439
Description: A use-after-free vulnerability during XSLT processing due to poor handling of template parameters. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1336830

Reference: CVE-2017-5440
Description: A use-after-free vulnerability during XSLT processing due to a failure to propagate error conditions during matching while evaluating context, leading to objects being used when they no longer exist. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1336832

Reference: CVE-2017-5441
Description: A use-after-free vulnerability when holding a selection during scroll events. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1343795

seebug
Reference: CVE-2017-5447
Description: Mozilla Firefox: out-of-bounds read in gfxTextRun(CVE-2017-5447)
Link: https://www.seebug.org/vuldb/ssvid-93154

Reference: CVE-2017-5465
Description: Mozilla Firefox: Memory disclosure in ConvolvePixel(CVE-2017-5465)
Link: https://www.seebug.org/vuldb/ssvid-93152

packetstorm
Reference: CVE-2017-5447
Description: Mozilla Firefox gfxTextRun Out-Of-Bounds Read
Link: https://packetstormsecurity.com/files/142668/Mozilla-Firefox-gfxTextRun-Out-Of-Bounds-Read.html

Reference: CVE-2017-5465
Description: Mozilla Firefox ConvolvePixel Memory Disclosure
Link: https://packetstormsecurity.com/files/142670/Mozilla-Firefox-ConvolvePixel-Memory-Disclosure.html

0day.today
Reference: CVE-2017-5447

Description: Mozilla Firefox < 53 - gfxTextRun Out-of-Bounds Read Exploit
Link: https://0day.today/exploit/27840

Reference: CVE-2017-5465
Description: Mozilla Firefox < 53 - ConvolvePixel Memory Disclosure Exploit
Link: https://0day.today/exploit/27839

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities. (mfsa2017-15,mfsa2017-16)

| | |
|---|---|
| QID: | 370431 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5470, CVE-2017-5471, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7755, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7759, CVE-2017-7760, CVE-2017-7761, CVE-2017-7762, CVE-2017-7763, CVE-2017-7764, CVE-2017-7765, CVE-2017-7766, CVE-2017-7767, CVE-2017-7768, CVE-2017-7770, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778 |
| Vendor Reference: | mfsa2017-15 to mfsa2017-16 |
| Bugtraq ID: | 99057,99052,99047,99049,99041,99042,99040 |
| Service Modified: | 07/29/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A local user can obtain elevated privileges on the target system. A local user can modify files on the target system. A remote user can obtain files on the target system. A remote user can spoof the address bar.
Affected Version :
Firefox prior to 54.0
Firefox ESR prior to 52.2

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A local
user can obtain elevated privileges on the target system.

A local user can modify files on the target system.

A remote user can obtain
files on the target system.

A remote user can spoof the address bar.

SOLUTION:

The vendor has issued a fix (ESR 52.2; 54.0). Refer to MFSA 2017-15 and MFSA 2017-16 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2017-15 and MFSA 2017-16: Windows (https://www.mozilla.org/en-US/security/advisories/)
MFSA 2017-15 and MFSA 2017-16: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd
Reference: CVE-2017-7750

Description: A use-after-free vulnerability during video control operations when a "" element holds a reference to an older window if that window has been replaced in the DOM. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1356558

Reference: CVE-2017-7751

Description: A use-after-free vulnerability with content viewer listeners that results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1363396

Reference: CVE-2017-7754

Description: An out-of-bounds read in WebGL with a maliciously crafted "ImageInfo" object during WebGL operations. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1357090

Reference: CVE-2017-7758

Description: An out-of-bounds read vulnerability with the Opus encoder when the number of channels in an audio stream changes while the encoder is in use. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1368490

Reference: CVE-2017-7759

Description: Android intent URLs given to Firefox for Android can be used to navigate from HTTP or HTTPS URLs to local "file:" URLs, allowing for the reading of local data through a violation of same-origin policy. Note: This attack only affects Firefox for Android. Other operating systems are not affected. This vulnerability affects Firefox < 54.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1356893

Reference: CVE-2017-7760

Description: The Mozilla Windows updater modifies some files to be updated by reading the original file and applying changes to it. The location of the original file can be altered by a malicious user by passing a special path to the callback parameter through the Mozilla Maintenance Service, allowing the manipulation of files in the installation directory and privilege escalation by manipulating the Mozilla Maintenance Service, which has privileged access. Note: This attack requires local system access and

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1348645

Reference: CVE-2017-7762

Description: When entered directly, Reader Mode did not strip the username and password section of URLs displayed in the addressbar. This can be used for spoofing the domain of the current page. This vulnerability affects Firefox < 54.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1358248

Reference: CVE-2017-7764

Description: Characters from the "Canadian Syllabics" unicode block can be mixed with characters from other unicode blocks in the addressbar instead of being rendered as their raw "punycode" form, allowing for domain name spoofing attacks through character confusion. The current Unicode standard allows characters from "Aspirational Use Scripts" such as Canadian Syllabics to be mixed with Latin characters in the "moderately restrictive" IDN profile. We have changed Firefox behavior to match the upcoming Unico

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1364283

Reference: CVE-2017-7771

Description: Out-of-bounds read in Graphite2 Library in Firefox before 54 in graphite2::Pass::readPass function.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Reference: CVE-2017-7772

Description: Heap-based Buffer Overflow in Graphite2 library in Firefox before 54 in lz4::decompress function.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Reference: CVE-2017-7773

Description: Heap-based Buffer Overflow write in Graphite2 library in Firefox before 54 in lz4::decompress src/Decompressor.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Reference: CVE-2017-7774

Description: Out-of-bounds read in Graphite2 Library in Firefox before 54 in graphite2::Silf::readGraphite function.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Reference: CVE-2017-7776

Description: Heap-based Buffer Overflow read in Graphite2 library in Firefox before 54 in graphite2::Silf::getClassGlyph.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Reference: CVE-2017-7777
Description: Use of uninitialized memory in Graphite2 library in Firefox before 54 in graphite2::GlyphCache::Loader::read_glyph function.
Link: https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities. (mfsa2017-18,mfsa2017-19)

| | |
|---|---|
| QID: | 370507 |
| Category: | Local |
| Associated CVEs: | CVE-2017-7753, CVE-2017-7779, CVE-2017-7780, CVE-2017-7781, CVE-2017-7782, CVE-2017-7783, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7788, CVE-2017-7789, CVE-2017-7790, CVE-2017-7791, CVE-2017-7792, CVE-2017-7794, CVE-2017-7796, CVE-2017-7797, CVE-2017-7798, CVE-2017-7799, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7804, CVE-2017-7806, CVE-2017-7807, CVE-2017-7808, CVE-2017-7809 |
| Vendor Reference: | mfsa2017-18 to mfsa2017-19 |
| Bugtraq ID: | 100198,100377,100196,100202,100197,100234,100206,100389,100242,100373,100203,100379,100374,100240,100315,100201,100199,100383,10024 |
| Service Modified: | 05/30/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can cause denial of service conditions on the target system. A remote user can bypass security controls on the target system. A remote user can obtain potentially sensitive information on the target system. A remote user can spoof content. A remote user can conduct cross-site scripting attacks.
Affected Version :
Firefox prior to 55.0
Firefox ESR prior to 52.3

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote
user can cause denial of service conditions.

A remote user can bypass security controls on the target system.

A remote user can obtain
potentially sensitive information on the target system.

A remote user can spoof content.

A remote user can access the target user's
cookies (including authentication cookies), if any, associated with an arbitrary site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

SOLUTION:

The vendor has issued a fix (55.0) and 52.3 ESR
Refer to MFSA 2017-18 and MFSA 2017-19 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-18 to mfsa2017-19: Windows (https://www.mozilla.org/en-US/security/advisories/)
mfsa2017-18 to mfsa2017-19: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2017-7783
Description: Mozilla Firefox < 55 - Denial of Service - The Exploit-DB Ref : 43020
Link: http://www.exploit-db.com/exploits/43020

exploitdb
Reference: CVE-2017-7783
Description: Mozilla Firefox < 55 - Denial of Service
Link: https://www.exploit-db.com/exploits/43020

nvd
Reference: CVE-2017-7753
Description: An out-of-bounds read occurs when applying style rules to pseudo-elements, such as ::first-line, using cached style data. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1353312

Reference: CVE-2017-7781
Description: An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it can yield a result "POINT_AT_INFINITY" when it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attacked party computing an incorrect shared secret. This vulnerability affects Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1352039

Reference: CVE-2017-7784
Description: A use-after-free vulnerability can occur when reading an image observer during frame reconstruction after the observer has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1376087

Reference: CVE-2017-7785
Description: A buffer overflow can occur when manipulating Accessible Rich Internet Applications (ARIA) attributes within the DOM. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1356985

Reference: CVE-2017-7786
Description: A buffer overflow can occur when the image renderer attempts to paint non-displayable SVG elements. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1365189

Reference: CVE-2017-7787
Description: Same-origin policy protections can be bypassed on pages with embedded iframes during page reloads, allowing the iframes to access content on the top level page, leading to information disclosure. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1322896

Reference: CVE-2017-7788
Description: When an "iframe" has a "sandbox" attribute and its content is specified using "srcdoc", that content does not inherit the containing page's Content Security Policy (CSP) as it should unless the sandbox attribute included "allow-same-origin". This vulnerability affects Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1073952

Reference: CVE-2017-7797
Description: Response header name interning does not have same-origin protections and these headers are stored in a global registry. This allows stored header names to be available cross-origin. This vulnerability affects Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1334776

Reference: CVE-2017-7799
Description: JavaScript in the "about:webrtc" page is not sanitized properly being assigned to "innerHTML". Data on this page is supplied by WebRTC usage and is not under third-party control, making this difficult to exploit, but the vulnerability could possibly be used for a cross-site scripting (XSS) attack. This vulnerability affects Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1372509

Reference: CVE-2017-7800
Description: A use-after-free vulnerability can occur in WebSockets when the object holding the connection is freed before the disconnection operation is finished. This results in an exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1374047

Reference: CVE-2017-7801
Description: A use-after-free vulnerability can occur while re-computing layout for a "marquee" element during window resizing where the updated style object

is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1371259

Reference: CVE-2017-7802

Description: A use-after-free vulnerability can occur when manipulating the DOM during the resize event of an image element. If these elements have been freed due to a lack of strong references, a potentially exploitable crash may occur when the freed elements are accessed. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1378147

Reference: CVE-2017-7803

Description: When a page's content security policy (CSP) header contains a "sandbox" directive, other directives are ignored. This results in the incorrect enforcement of CSP. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1377426

Reference: CVE-2017-7806

Description: A use-after-free vulnerability can occur when the layer manager is freed too early when rendering specific SVG content, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1378113

Reference: CVE-2017-7807

Description: A mechanism that uses AppCache to hijack a URL in a domain using fallback by serving the files from a sub-path on the domain. This has been addressed by requiring fallback files be inside the manifest directory. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1376459

Reference: CVE-2017-7809

Description: A use-after-free vulnerability can occur when an editor DOM node is deleted prematurely during tree traversal while still bound to the document. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1380284

Reference: CVE-2017-7789

Description: If a server sends two Strict-Transport-Security (STS) headers for a single connection, they will be rejected as invalid and HTTP Strict Transport Security (HSTS) will not be enabled for the connection. This vulnerability affects Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1074642

Reference: CVE-2017-7791

Description: On pages containing an iframe, the "data:" protocol can be used to create a modal alert that will render over arbitrary domains following page navigation, spoofing of the origin of the modal alert from the iframe content. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1365875

Reference: CVE-2017-7792

Description: A buffer overflow will occur when viewing a certificate in the certificate manager if the certificate has an extremely long object identifier (OID). This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1368652

Reference: CVE-2017-7794

Description: On Linux systems, if the content process is compromised, the sandbox broker will allow files to be truncated even though the sandbox explicitly only has read access to the local file system and no write permissions. Note: This attack only affects the Linux operating system. Other operating systems are not affected. This vulnerability affects Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1374281

Reference: CVE-2017-7783

Description: If a long user name is used in a username/password combination in a site URL (such as " http://UserName:Password@example.com"), the resulting modal prompt will hang in a non-responsive state or crash, causing a denial of service. This vulnerability affects Firefox < 55.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1360842

packetstorm

Reference: CVE-2017-7783

Description: Mozilla Firefox Username Denial Of Service

Link: https://packetstormsecurity.com/files/144687/Mozilla-Firefox-Username-Denial-Of-Service.html

0day.today

Reference: CVE-2017-7783

Description: Mozilla Firefox < 55 - Denial of Service Exploit
Link: https://0day.today/exploit/28828

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities. (mfsa2017-21,mfsa2017-22)

| | |
|---|---|
| QID: | 370584 |
| Category: | Local |
| Associated CVEs: | CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7811, CVE-2017-7812, CVE-2017-7813, CVE-2017-7814, CVE-2017-7815, CVE-2017-7816, CVE-2017-7817, CVE-2017-7818, CVE-2017-7819, CVE-2017-7820, CVE-2017-7821, CVE-2017-7822, CVE-2017-7823, CVE-2017-7824, CVE-2017-7825 |
| Vendor Reference: | mfsa2017-21 and mfsa2017-22 |
| Bugtraq ID: | 101054,101055,101059,101057,101053 |
| Service Modified: | 05/30/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can obtain potentially sensitive information on the target system. A remote user can spoof URLs. A remote user can conduct cross-site scripting attacks.
Affected Versions :
Firefox prior to 56.0
Firefox ESR prior to 52.4

IMPACT:

A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user's system.

A remote
user can obtain potentially sensitive information on the target system.

A remote user can spoof the address bar and other user interface
components.

A remote user can conduct cross-site scripting attacks.

SOLUTION:

The vendor has issued a fix (56.0, 52.4ESR).
Refer to MFSA 2017-21 and MFSA 2017-22 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2017-21 and MFSA 2017-22: Windows (https://www.mozilla.org/en-US/security/advisories/)
MFSA 2017-21 and MFSA 2017-22: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2017-7811
Description: Memory safety bugs were reported in Firefox 55. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 56.
Link:
https://bugzilla.mozilla.org/buglist.cgi?bug_id=1392105%2C1395919%2C1388113%2C1348955%2C1394522%2C1387659%2C1369560%2C1388045%

Reference: CVE-2017-7812
Description: If web content on a page is dragged onto portions of the browser UI, such as the tab bar, links can be opened that otherwise would not be allowed

to open. This can allow malicious web content to open a locally stored file through "file:" URLs. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1379842

Reference: CVE-2017-7813

Description: Inside the JavaScript parser, a cast of an integer to a narrower type can result in data read from outside the buffer being parsed. This usually results in a non-exploitable crash, but can leak a limited amount of information from memory if it matches JavaScript identifier syntax. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1383951

Reference: CVE-2017-7815

Description: On pages containing an iframe, the "data:" protocol can be used to create a modal dialog through Javascript that will have an arbitrary domains as the dialog's location, spoofing of the origin of the modal dialog from the user view. Note: This attack only affects installations with e10 multiprocess turned off. Installations with e10s turned on do not support the modal dialog functionality. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1368981

Reference: CVE-2017-7816

Description: WebExtensions could use popups and panels in the extension UI to load an "about:" privileged URL, violating security checks that disallow this behavior. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1380597

Reference: CVE-2017-7817

Description: A spoofing vulnerability can occur when a page switches to fullscreen mode without user notification, allowing a fake address bar to be displayed. This allows an attacker to spoof which page is actually loaded and in use. Note: This attack only affects Firefox for Android. Other operating systems are not affected. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1356596

Reference: CVE-2017-7818

Description: A use-after-free vulnerability can occur when manipulating arrays of Accessible Rich Internet Applications (ARIA) elements within containers through the DOM. This results in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1363723

Reference: CVE-2017-7819

Description: A use-after-free vulnerability can occur in design mode when image objects are resized if objects referenced during the resizing have been freed from memory. This results in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1380292

Reference: CVE-2017-7820

Description: The "instanceof" operator can bypass the Xray wrapper mechanism. When called on web content from the browser itself or an extension the web content can provide its own result for that operator, possibly tricking the browser or extension into mishandling the element. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1378207

Reference: CVE-2017-7821

Description: A vulnerability where WebExtensions can download and attempt to open a file of some non-executable file types. This can be triggered without specific user interaction for the file download and open actions. This could be used to trigger known vulnerabilities in the programs that handle those document types. This vulnerability affects Firefox < 56.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1346515

Reference: CVE-2017-7823

Description: The content security policy (CSP) "sandbox" directive did not create a unique origin for the document, causing it to behave as if the "allow-same-origin" keyword were always specified. This could allow a Cross-Site Scripting (XSS) attack to be launched from unsafe content. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1396320

0day.today

Reference: CVE-2017-7821

Description: Firefox browser.downloads addon Remote Code Execute (PoC) Vulnerability

Link: https://0day.today/exploit/28675

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities. (mfsa2017-24,mfsa2017-25)

| | |
|---|---|
| QID: | 370658 |
| Category: | Local |
| Associated CVEs: | CVE-2017-7828, CVE-2017-7830, CVE-2017-7826, CVE-2017-7831, CVE-2017-7832, CVE-2017-7833, CVE-2017-7834, CVE-2017-7835, CVE-2017-7836, CVE-2017-7837, CVE-2017-7838, CVE-2017-7839, CVE-2017-7840, CVE-2017-7842, CVE-2017-7827 |
| Vendor Reference: | mfsa2017-24 and mfsa2017-25 |
| Bugtraq ID: | 101832 |
| Service Modified: | 11/16/2017 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.Cross-origin URL information leak through Resource Timing API.Information disclosure of exposed properties on JavaScript proxy objects.Domain spoofing through use of dotless 'i' character followed by accent markers.URLs opened in new tabs bypass CSP protections.Pingsender dynamically loads libcurl on Linux and OS X.Control characters before javascript: URLs defeats self-XSS prevention mechanism.Exported bookmarks do not strip script elements from user-supplied tags.
Affected Versions:
Firefox prior to 57.0
Firefox ESR prior to 52.5

IMPACT:

Cross-origin URL information leak through Resource Timing API.

Information disclosure of exposed properties on JavaScript proxy objects.

Domain spoofing through use of dotless 'i' character followed by accent markers.

URLs opened in new tabs bypass CSP protections.

Pingsender dynamically loads libcurl on Linux and OS X.

Control characters before javascript: URLs defeats self-XSS prevention mechanism.

Exported bookmarks do not strip script elements from user-supplied tags.

SOLUTION:

The vendor has issued a fix (57.0, 52.5ESR).
Refer to MFSA 2017-24 and MFSA 2017-25 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2017-24 and MFSA 2017-25: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
MFSA 2017-24 and MFSA 2017-25: Windows (https://www.mozilla.org/en-US/security/advisories/)

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 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (mfsa2017-28,mfsa2017-29)

| | |
|---|---|
| QID: | 370679 |
| Category: | Local |
| Associated CVEs: | CVE-2017-7843, CVE-2017-7845 |
| Vendor Reference: | mfsa2017-28 and mfsa2017-29 |
| Bugtraq ID: | 102039,102112,102115 |
| Service Modified: | 05/30/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.Buffer overflow when drawing and validating elements with ANGLE library using Direct 3D 9.Web worker in Private Browsing mode can write IndexedDB data.
Affected Versions:
Firefox prior to 57.0.2
Firefox ESR prior to 52.5.2

IMPACT:

Buffer overflow when drawing and validating elements with ANGLE library using Direct 3D 9.

Web worker in Private Browsing mode can write
IndexedDB data.

SOLUTION:

The vendor has issued a fix (57.0.2, 52.5.2 ESR).
Refer to MFSA 2017-28 and MFSA 2017-29 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2017-28 and MFSA 2017-29: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
MFSA 2017-28 and MFSA 2017-29: Windows (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

| | |
|---|---|
| Reference: | CVE-2017-7843 |
| Description: | When Private Browsing mode is used, it is possible for a web worker to write persistent data to IndexedDB and fingerprint a user uniquely. IndexedDB should not be available in Private Browsing mode and this stored data will persist across multiple private browsing mode sessions because it is not cleared when exiting. This vulnerability affects Firefox ESR < 52.5.2 and Firefox < 57.0.1. |
| Link: | https://bugzilla.mozilla.org/show_bug.cgi?id=1410106 |

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA-2018-20,MFSA-2018-21)

| | |
|---|---|
| QID: | 371173 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12377, CVE-2018-12378, CVE-2018-12379, CVE-2017-16541, CVE-2018-12381, CVE-2018-12382, CVE-2018-12383, CVE-2018-12375, CVE-2018-12376, CVE-2018-18499 |
| Vendor Reference: | MFSA2018-20, MFSA2018-21 |
| Bugtraq ID: | 101665,105276,105280 |
| Service Modified: | 05/30/2023 |
| 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.
CVE-2018-12377: Use-after-free in refresh driver timers

CVE-2018-12378: Use-after-free in IndexedDB

CVE-2018-12379: Out-of-bounds write with malicious MAR file

CVE-2017-16541: Proxy bypass using automount and autofs

CVE-2018-12381: Dragging and dropping Outlook email message results in page navigation

CVE-2018-12382: Addressbar spoofing with javascript URI on Firefox for Android

CVE-2018-12383: Setting a master password post-Firefox 58 does not delete unencrypted previously stored passwords

CVE-2018-12375: Memory safety bugs fixed in Firefox 62

CVE-2018-12376: Memory safety bugs fixed in Firefox 62 and Firefox ESR 60.2
Affected Products :
Prior to Firefox 62
Prior to Firefox ESR 60.2

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2018-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-20) and MFSA2018-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-21) .
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2018-20: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-20)
MFSA2018-20: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-20)
MFSA2018-21: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-21)
MFSA2018-21: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-21)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2017-16541
Description: Tor Browser before 7.0.9 on macOS and Linux allows remote attackers to bypass the intended anonymity feature and discover a client IP address via vectors involving a crafted web site that leverages file:// mishandling in Firefox, aka TorMoil. NOTE: Tails is unaffected.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1412081

Reference: CVE-2018-12382
Description: The displayed addressbar URL can be spoofed on Firefox for Android using a javascript: URI in concert with JavaScript to insert text before the loaded domain name, scrolling the loaded domain out of view to the right. This can lead to user confusion. *This vulnerability only affects Firefox for Android < 62.*
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1479311

Reference: CVE-2018-12383
Description: If a user saved passwords before Firefox 58 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Firefox 58. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. This vulnerability affects Firefox < 62, Firefox ESR < 60.2.1, and Thunderbird < 60.2.1.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1475775

packetstorm

Reference: CVE-2017-16541
Description: Tor Browser 7.0.8 Information Disclosure
Link: https://packetstormsecurity.com/files/149298/Tor-Browser-7.0.8-Information-Disclosure.html

0day.today

Reference: CVE-2017-16541
Description: Tor Browser 7.0.8 Information Disclosure Vulnerability
Link: https://0day.today/exploit/31069

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-22,MFSA2018-23)

| | |
|---|---|
| QID: | 371216 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12385, CVE-2018-12383 |
| Vendor Reference: | MFSA2018-22, MFSA2018-23 |
| Bugtraq ID: | 105276,105380 |
| Service Modified: | 05/30/2023 |
| 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.
CVE-2018-12385: Crash in TransportSecurityInfo due to cached data.
CVE-2018-12383: Setting a master password post-Firefox 58 does not delete unencrypted previously stored passwords.
Affected Products:
Prior to Firefox 62.0.2
Prior to Firefox ESR 60.2.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2018-22 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-22) and MFSA2018-23 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-23/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2018-22: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-22)
MFSA2018-22: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-22)
MFSA2018-23: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-23/)
MFSA2018-23: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-23/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2018-12383
Description: If a user saved passwords before Firefox 58 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Firefox 58. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. This vulnerability affects Firefox < 62, Firefox ESR < 60.2.1, and Thunderbird < 60.2.1.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1475775

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 5 Mozilla Firefox and Firefox ESR Type Confusion Vulnerability (MFSA2019-18)

| | |
|---|---|
| QID: | 371849 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11707 |
| Vendor Reference: | MFSA2019-18 |
| Bugtraq ID: | - |
| Service Modified: | 11/15/2023 |
| 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.
CVE-2019-11707: Type confusion in Array.pop
Affected Products: Prior to Firefox 67.0.3 and Firefox ESR 60.7.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-18 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-18)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-18: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-18)
MFSA2019-18: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-18)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2019-11707
Description: Mozilla Spidermonkey - IonMonkey 'Array.prototype.pop' Type Confusion - The Exploit-DB Ref : 47038
Link: http://www.exploit-db.com/exploits/47038

Reference: CVE-2019-11707
Description: Mozilla Firefox 67 - Array.pop JIT Type Confusion - The Exploit-DB Ref : 50691
Link: http://www.exploit-db.com/exploits/50691

exploitdb

Reference: CVE-2019-11707
Description: Mozilla Firefox 67 - Array.pop JIT Type Confusion
Link: https://www.exploit-db.com/exploits/50691

Reference: CVE-2019-11707
Description: Mozilla Spidermonkey - IonMonkey 'Array.prototype.pop' Type Confusion
Link: https://www.exploit-db.com/exploits/47038

packetstorm

Reference: CVE-2019-11707
Description: Spidermonkey IonMonkey Incorrect Prediction
Link: https://packetstormsecurity.com/files/153422/Spidermonkey-IonMonkey-Incorrect-Prediction.html

Reference: CVE-2019-11707
Description: Mozilla Firefox 67 Array.pop JIT Type Confusion

Link: https://packetstormsecurity.com/files/165816/Mozilla-Firefox-67-Array.pop-JIT-Type-Confusion.html

0day.today

Reference: CVE-2019-11707
Description: Mozilla Spidermonkey - IonMonkey (Array.prototype.pop) Type Confusion Exploit
Link: https://0day.today/exploit/32912

Reference: CVE-2019-11707
Description: Mozilla Firefox 67 - Array.pop JIT Type Confusion Exploit
Link: https://0day.today/exploit/37293

github-exploits

Reference: CVE-2019-11707
Description: tunnelshade/cve-2019-11707 exploit repository
Link: https://github.com/tunnelshade/cve-2019-11707

Reference: CVE-2019-11707
Description: vigneshsrao/CVE-2019-11707 exploit repository
Link: https://github.com/vigneshsrao/CVE-2019-11707

cisa-kev

Reference: CVE-2019-11707
Description: Mozilla Firefox and Thunderbird Type Confusion Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2019-11707
Description: Mozilla Firefox Type confusion in Array.pop
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

issue-tracker

Reference: CVE-2019-11707
Description: Issue 1820: Spidermonkey: IonMonkey incorrectly predicts return type of Array.prototype.pop, leading to type confusions
Link: https://bugs.chromium.org/p/project-zero/issues/detail?id=1820

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2019-25)(MFSA2019-26)(MFSA2019-27)

| | |
|---|---|
| QID: | 372102 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11751, CVE-2019-11746, CVE-2019-11744, CVE-2019-11742, CVE-2019-11736, CVE-2019-11753, CVE-2019-11752, CVE-2019-9812, CVE-2019-11741, CVE-2019-11743, CVE-2019-11748, CVE-2019-11749, CVE-2019-5849, CVE-2019-11750, CVE-2019-11737, CVE-2019-11738, CVE-2019-11747, CVE-2019-11734, CVE-2019-11735, CVE-2019-11740 |
| Vendor Reference: | MFSA2019-25, MFSA2019-26, MFSA2019-27 |
| Bugtraq ID: | - |
| Service Modified: | 05/30/2023 |
| 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.
CVE-2019-11751: Malicious code execution through command line parameters.

CVE-2019-11746: Use-after-free while manipulating video

CVE-2019-11744: XSS by breaking out of title and textarea elements using innerHTML

CVE-2019-11742: Same-origin policy violation with SVG filters and canvas to steal cross-origin images

CVE-2019-11736: File manipulation and privilege escalation in Mozilla Maintenance Service

CVE-2019-11753: Privilege escalation with Mozilla Maintenance Service in custom Firefox installation location

CVE-2019-11752: Use-after-free while extracting a key value in IndexedDB

CVE-2019-9812: Sandbox escape through Firefox Sync

CVE-2019-11741: Isolate addons.mozilla.org and accounts.firefox.com

CVE-2019-11743: Cross-origin access to unload event attributes

CVE-2019-11748: Persistence of WebRTC permissions in a third party context

CVE-2019-11749: Camera information available without prompting using getUserMedia

CVE-2019-5849: Out-of-bounds read in Skia

CVE-2019-11750: Type confusion in Spidermonkey

CVE-2019-11737: Content security policy directives ignore port and path if host is a wildcard

CVE-2019-11738: Content security policy bypass through hash-based sources in directives

CVE-2019-11747: 'Forget about this site' removes sites from pre-loaded HSTS list

CVE-2019-11734: Memory safety bugs fixed in Firefox 69

CVE-2019-11735: Memory safety bugs fixed in Firefox 69 and Firefox ESR 68.1

CVE-2019-11740: Memory safety bugs fixed in Firefox 69, Firefox ESR 68.1, and Firefox ESR 60.9
Affected Products : Prior to Firefox 69, Firefox ESR 68.1, and Firefox ESR 60.9

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-25 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-25)
MFSA2019-26 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-26)
MFSA2019-27 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-27)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-25: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-25)
MFSA2019-25: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-25)
MFSA2019-26 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-26)
MFSA2019-27 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-27)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-11743

Description: Navigation events were not fully adhering to the W3C's "Navigation-Timing Level 2" draft specification in some instances for the unload event, which restricts access to detailed timing attributes to only be same-origin. This resulted in potential cross-origin information exposure of history through timing side-channel attacks. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.

Link: https://w3c.github.io/navigation-timing

Reference: CVE-2019-11738

Description: If a Content Security Policy (CSP) directive is defined that uses a hash-based source that takes the empty string as input, execution of any javascript: URIs will be allowed. This could allow for malicious JavaScript content to be run, bypassing CSP permissions. This vulnerability affects Firefox < 69 and Firefox ESR < 68.1.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1452037

Reference: CVE-2019-5849

Description: Out of bounds read in Skia in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.

Link: https://crbug.com/954891

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox and Firefox ESR Multiple Vulnerabilities (MFSA 2019-36,MFSA 2019-37)

| | |
|---|---|
| QID: | 372276 |
| Category: | Local |
| Associated CVEs: | CVE-2019-17008, CVE-2019-13722, CVE-2019-11745, CVE-2019-17009, CVE-2019-17010, CVE-2019-17005, CVE-2019-17011, CVE-2019-17012, CVE-2019-11756, CVE-2019-17014, CVE-2019-17013 |
| Vendor Reference: | MFSA2019-36, MSFA2019-37 |
| Bugtraq ID: | - |
| Service Modified: | 08/07/2023 |
| 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.
CVE-2019-17008: Use-after-free in worker destruction

CVE-2019-13722: Stack corruption due to incorrect number of arguments in WebRTC code

CVE-2019-11745: Out of bounds write in NSS when encrypting with a block cipher

CVE-2019-17009: Updater temporary files accessible to unprivileged processes

CVE-2019-17010: Use-after-free when performing device orientation checks

CVE-2019-17005: Buffer overflow in plain text serializer

CVE-2019-17011: Use-after-free when retrieving a document in antitracking

CVE-2019-17012: Memory safety bugs fixed in Firefox 71 and Firefox ESR 68.3

CVE-2019-17008: Use-after-free in worker destruction

CVE-2019-17014: Dragging and dropping a cross-origin resource, incorrectly loaded as an image, could result in information disclosure

CVE-2019-17013: Memory safety bugs fixed in Firefox 71
Affected Products : Prior to - Firefox 71
Affected Products : Prior to - Firefox ESR 68.3

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-36 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-36) and MFSA2019-37 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-37)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-36: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-36)
MFSA2019-36: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-36)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-17005
Description: The plain text serializer used a fixed-size array for the number of elements it could process; however it was possible to overflow the static-sized array leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1584170

Reference: CVE-2019-17010
Description: Under certain conditions, when checking the Resist Fingerprinting preference during device orientation checks, a race condition could have caused a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1581084

Reference: CVE-2019-17011
Description: Under certain conditions, when retrieving a document from a DocShell in the antitracking code, a race condition could cause a use-after-free condition and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1591334

Reference: CVE-2019-17013
Description: Mozilla developers reported memory safety bugs present in Firefox 70. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 71.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1298509%2C1472328%2C1577439%2C1577937%2C1580320%2C1584195%2C1585106%2C1586293%

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox and Firefox ESR Multiple Vulnerabilities (MFSA2020-01,MFSA2020-02)

| | |
|---|---|
| QID: | 372324 |
| Category: | Local |
| Associated CVEs: | CVE-2019-17015, CVE-2019-17016, CVE-2019-17017, CVE-2019-17018, CVE-2019-17019, CVE-2019-17020, CVE-2019-17021, CVE-2019-17022, CVE-2019-17023, CVE-2019-17024, CVE-2019-17025 |
| Vendor Reference: | MFSA2020-01, MFSA2020-02 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2019-17015: Memory corruption in parent process during new content process initialization on Windows
CVE-2019-17016: Bypass of @namespace CSS sanitization during pasting
CVE-2019-17017: Type Confusion in XPCVariant.cpp
CVE-2019-17018: Windows Keyboard in Private Browsing Mode may retain word suggestions
CVE-2019-17019: Python files could be inadvertently executed upon opening a download
CVE-2019-17020: Content Security Policy not applied to XSL stylesheets applied to XML documents
CVE-2019-17021: Heap address disclosure in parent process during content process initialization on Windows
CVE-2019-17022: CSS sanitization does not escape HTML tags
CVE-2019-17023: NSS may negotiate TLS 1.2 or below after a TLS 1.3 HelloRetryRequest had been sent
CVE-2019-17024: Memory safety bugs fixed in Firefox 72 and Firefox ESR 68.4
CVE-2019-17025: Memory safety bugs fixed in Firefox 72
Affected Products : Prior to - Firefox 72
Affected Products : Prior to - Firefox ESR 68.4

IMPACT:

On successful exploitation it could allow an attacker to run arbitrary code,lead to memory corruption and a potentially exploitable crash or disclose heap addresses from the parent process.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to mfsa2020-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-01/#CVE-2019-17024) and MFSA2020-02 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-02/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-01,MFSA2020-02: Windows,Linux
(https://www.mozilla.org/en-US/security/advisories/mfsa2020-01/#CVE-2019-17024,https://www.mozilla.org/en-US/security/advisories/mfsa2020-02/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-17021
Description: During the initialization of a new content process, a race condition occurs that can allow a content process to disclose heap addresses from the parent process. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1599008

Reference: CVE-2019-17021
Description: During the initialization of a new content process, a race condition occurs that can allow a content process to disclose heap addresses from the parent process. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
Link: http://packetstormsecurity.com/files/155912/Slackware-Security-Advisory-mozilla-thunderbird-Updates.html

Reference: CVE-2019-17024
Description: Mozilla developers reported memory safety bugs present in Firefox 71 and Firefox ESR 68.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
Link: http://packetstormsecurity.com/files/155912/Slackware-Security-Advisory-mozilla-thunderbird-Updates.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox and Firefox ESR StoreElementHole and FallibleStoreElement Vulnerability (MFSA2020-03)

| | |
|---|---|
| QID: | 372325 |
| Category: | Local |
| Associated CVEs: | CVE-2019-17026 |
| Vendor Reference: | MFSA2020-03 |

| | |
|---|---|
| Bugtraq ID: | - |
| Service Modified: | 07/25/2023 |
| 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.
CVE-2019-17026: IonMonkey type confusion with StoreElementHole and FallibleStoreElement
Affected Products : Prior to Firefox 72.0.1 and Firefox ESR 68.4.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-03 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-03)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-03: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2020-03)
MFSA2020-03: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2020-03)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2019-17026
- Description: Firefox 72 IonMonkey - JIT Type Confusion - The Exploit-DB Ref : 49864
- Link: http://www.exploit-db.com/exploits/49864

exploitdb
- Reference: CVE-2019-17026
- Description: Firefox 72 IonMonkey - JIT Type Confusion
- Link: https://www.exploit-db.com/exploits/49864

nvd
- Reference: CVE-2019-17026
- Description: Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 68.4.1, Thunderbird < 68.4.1, and Firefox < 72.0.1.
- Link: http://packetstormsecurity.com/files/162568/Firefox-72-IonMonkey-JIT-Type-Confusion.html

packetstorm
- Reference: CVE-2019-17026
- Description: Firefox 72 IonMonkey JIT Type Confusion
- Link: https://packetstormsecurity.com/files/162568/Firefox-72-IonMonkey-JIT-Type-Confusion.html

0day.today
- Reference: CVE-2019-17026
- Description: Mozilla Firefox 72 IonMonkey - JIT Type Confusion Exploit
- Link: https://0day.today/exploit/36241

github-exploits
- Reference: CVE-2019-17026
- Description: maxpl0it/CVE-2019-17026-Exploit exploit repository
- Link: https://github.com/maxpl0it/CVE-2019-17026-Exploit

cisa-kev
- Reference: CVE-2019-17026
- Description: Mozilla Firefox IonMonkey JIT compiler Type Confusion Vulnerability
- Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2019-17026
Description: Mozilla Firefox Type confusion in IonMonkey JIT compiler
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2019-17026
Description: CVE-2019-17026: Firefox Type Confusion in IonMonkey
Link: https://googleprojectzero.github.io/0days-in-the-wild/0day-RCAs/2020/CVE-2019-17026.html

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2019-17026
Type: Exploit
Platform: Script,Win32

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-05,MFSA2020-06)

| | |
|---|---|
| QID: | 372392 |
| Category: | Local |
| Associated CVEs: | CVE-2020-6796, CVE-2020-6797, CVE-2020-6798, CVE-2020-6799, CVE-2020-6800, CVE-2020-6801 |
| Vendor Reference: | MFSA2020-05, MFSA2020-06 |
| Bugtraq ID: | - |
| Service Modified: | 07/27/2023 |
| 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.
CVE-2020-6796: Missing bounds check on shared memory read in the parent process
CVE-2020-6797: Extensions granted downloads.open permission could open arbitrary applications on Mac OSX
CVE-2020-6798: Incorrect parsing of template tag could result in JavaScript injection
CVE-2020-6799: Arbitrary code execution when opening pdf links from other applications, when Firefox is configured as default pdf reader
CVE-2020-6800: Memory safety bugs fixed in Firefox 73 and Firefox ESR 68.5
CVE-2020-6801: Memory safety bugs fixed in Firefox 73
Affected Products :
Prior to Firefox 73, Firefox ESR 68.5

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-05/)
MFSA2020-06 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-06/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-05/)
MFSA2020-06 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-06/)
MFSA2020-07 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-07/)

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  1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-45)

| | |
|---|---|
| QID: | 373542 |
| Category: | Local |
| Associated CVEs: | CVE-2020-15969, CVE-2020-15254, CVE-2020-15680, CVE-2020-15681, CVE-2020-15682, CVE-2020-15683, CVE-2020-15684 |
| Vendor Reference: | MFSA2020-45 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2020-15969: Use-after-free in usersctp

CVE-2020-15254: Undefined behavior in bounded channel of crossbeam rust crate

CVE-2020-15680: Presence of external protocol handlers could be determined through image tags

CVE-2020-15681: Multiple WASM threads may have overwritten each others' stub table entries

CVE-2020-15682: The domain associated with the prompt to open an external protocol could be spoofed to display the incorrect origin

CVE-2020-15683: Memory safety bugs fixed in Firefox 82 and Firefox ESR 78.4

CVE-2020-15684: Memory safety bugs fixed in Firefox 82
Affected Products : Prior to Firefox 82

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-45 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-45)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-45: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2020-45)
MFSA2020-45: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2020-45)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-15254
Description: Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect c
Link: https://github.com/crossbeam-rs/crossbeam/issues/539

Reference: CVE-2020-15254
Description: Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes

that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect c

Link: https://github.com/crossbeam-rs/crossbeam/pull/533

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-49)

| | |
|---|---|
| QID: | 373989 |
| Category: | Local |
| Associated CVEs: | CVE-2020-26950 |
| Vendor Reference: | MFSA2020-49 |
| Bugtraq ID: | - |
| Service Modified: | 08/15/2023 |
| 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.
CVE-2020-26950: Write side effects in MCallGetProperty opcode not accounted for
Affected Products : Prior to Firefox 82.0.3

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-49 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-49)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-49: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2020-49)
MFSA2020-49: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2020-49)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-26950
Description: In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1675905

Reference: CVE-2020-26950
Description: In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2.
Link: http://packetstormsecurity.com/files/166175/Firefox-MCallGetProperty-Write-Side-Effects-Use-After-Free.html

packetstorm

Reference: CVE-2020-26950
Description: Firefox MCallGetProperty Write Side Effects Use-After-Free
Link: https://packetstormsecurity.com/files/166175/Firefox-MCallGetProperty-Write-Side-Effects-Use-After-Free.html

metasploit

Reference: CVE-2020-26950
Description: Firefox MCallGetProperty Write Side Effects Use After Free Exploit

Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_jit_use_after_free.rb

Reference: CVE-2020-26950
Description: Firefox MCallGetProperty Write Side Effects Use After Free Exploit
Link: https://github.com/rapid7/metasploit-framework

0day.today
Reference: CVE-2020-26950
Description: Firefox MCallGetProperty Write Side Effects Use-After-Free Exploit
Link: https://0day.today/exploit/37440

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-54)

| | |
|---|---|
| QID: | 374576 |
| Category: | Local |
| Associated CVEs: | CVE-2020-16042, CVE-2020-26971, CVE-2020-26972, CVE-2020-26973, CVE-2020-26974, CVE-2020-26975, CVE-2020-26976, CVE-2020-26977, CVE-2020-26978, CVE-2020-26979, CVE-2020-35111, CVE-2020-35112, CVE-2020-35113, CVE-2020-35114 |
| Vendor Reference: | MFSA2020-54 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
Affected Products : Prior to Firefox 84.0

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-54 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-54)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-54 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd
Reference: CVE-2020-26979
Description: When a user typed a URL in the address bar or the search bar and quickly hit the enter key, a website could sometimes capture that event and then redirect the user before navigation occurred to the desired, entered address. To construct a convincing spoof the attacker would have had to guess what the user was typing, perhaps by suggesting it. This vulnerability affects Firefox < 84.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1641287%2C1673299

Reference: CVE-2020-35114
Description: Mozilla developers reported memory safety bugs present in Firefox 83. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84.

Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1607449%2C1640416%2C1656459%2C1669914%2C1673567

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

5 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-06)

| | |
|---|---|
| QID: | 375100 |
| Category: | Local |
| Associated CVEs: | CVE-2020-16048 |
| Vendor Reference: | MFSA2021-06 |
| Bugtraq ID: | - |
| Service Modified: | 11/05/2021 |
| 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 85.0.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-06 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-06/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-06 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-06/)

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 1.7.0.0

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  1.7.0.0

## 5 Microsoft Windows Curl Multiple Security Vulnerabilities

| | |
|---|---|
| QID: | 378936 |
| Category: | Local |
| Associated CVEs: | CVE-2023-38545, CVE-2023-38546 |
| Vendor Reference: | CVE-2023-38545 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Curl is a command-line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP, or FILE). curl is powered by Libcurl.
CVE-2023-38545:This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.
CVE-2023-38546:This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met.
Affected Versions:
CVE-2023-38545:libcurl from 7.69.0 prior to 8.4.0
CVE-2023-38546:libcurl from 7.9.1 prior to 8.4.0

IMPACT:

Successful exploitation makes curl overflow a heap based buffer in the SOCKS5 proxy handshake and also allows an attacker to insert cookies at will into a running program using libcurl.

SOLUTION:

curl has released fix to address this issue. Customers are advised to refer to CVE-2023-38545 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38545) for updates pertaining to this vulnerability.
Workaround:Note that after you have implemented any of the workarounds the file will still exist on disk, and can still be detected by scanning software. The workaround only provides an operating system level guarantee that the vulnerable version of the curl tool cannot be executed.
Workaround
Use a WDAC policy to deny execution of the \system32\curl.exe executable. You can merge the deny into an existing policy or create a new policy with it using the Merge-CIPolicy cmdlet; Merge-CIPolicy (ConfigCI) | Microsoft Learn. After the policy XML file with the deny has been created or merged with an existing policy it must be deployed.
For more information, please refer to CVE-2023-38545 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-38545)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2023-38545 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38545)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2023-38545
Description: dbrugman/CVE-2023-38545-POC exploit repository
Link: https://github.com/dbrugman/CVE-2023-38545-POC

Reference: CVE-2023-38545
Description: bcdannyboy/CVE-2023-38545 exploit repository
Link: https://github.com/bcdannyboy/CVE-2023-38545

Reference: CVE-2023-38545
Description: vanigori/CVE-2023-38545-sample exploit repository
Link: https://github.com/vanigori/CVE-2023-38545-sample

Reference: CVE-2023-38545
Description: UTsweetyfish/CVE-2023-38545 exploit repository
Link: https://github.com/UTsweetyfish/CVE-2023-38545

Reference: CVE-2023-38545
Description: fatmo666/CVE-2023-38545-libcurl-SOCKS5-heap-buffer-overflow exploit repository
Link: https://github.com/fatmo666/CVE-2023-38545-libcurl-SOCKS5-heap-buffer-overflow

Reference: CVE-2023-38545
Description: imfht/CVE-2023-38545 exploit repository
Link: https://github.com/imfht/CVE-2023-38545

gist

Reference: CVE-2023-38545
Description: CVE-2023-38545
Link: https://gist.github.com/xen0bit/0dccb11605abbeb6021963e2b1a811d3

blogs

Reference: CVE-2023-38545
Description: How I made a heap overflow in curl
Link: https://daniel.haxx.se/blog/2023/10/11/how-i-made-a-heap-overflow-in-curl/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%windir%\System32\curl.exe  Version is  8.0.1.0
%windir%\SysWOW64\curl.exe  Version is  8.0.1.0

### 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-2020-17078, CVE-2020-17079, CVE-2020-17081, CVE-2020-17082, CVE-2020-17086, CVE-2020-17101, CVE-2020-17102, CVE-2020-17105, CVE-2020-17106, CVE-2020-17107, CVE-2020-17108, CVE-2020-17109, CVE-2020-17110 |
| Bugtraq ID: | - |
| Service Modified: | 12/17/2021 |
| 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:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

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-2021-28464, CVE-2021-28466, 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 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-2021-31945, CVE-2021-31946, CVE-2021-31983 |
| Bugtraq ID: | - |
| Service Modified: | 08/02/2023 |
| 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 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-2022-21844, CVE-2022-21926, CVE-2022-21927, CVE-2022-22709 |
| 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-2022-22006, CVE-2022-22007, CVE-2022-23295, CVE-2022-23300, CVE-2022-23301, CVE-2022-24451, CVE-2022-24452, CVE-2022-24453, CVE-2022-24456, CVE-2022-24457, CVE-2022-24501 |
| 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 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: | 12/19/2023 |
| 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
Version '6.1907.29027.0'

4 Microsoft Windows Security Update for July 2023

| | |
|---|---|
| QID: | 92033 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-35366, CVE-2023-35309, CVE-2023-35306, CVE-2023-35305, CVE-2023-35304, CVE-2023-35303, CVE-2023-35302, CVE-2023-35299, CVE-2023-32053, CVE-2023-33174, CVE-2023-21526, CVE-2023-36871, CVE-2023-33155, CVE-2023-33154, CVE-2023-35308, CVE-2023-32055, CVE-2023-32054, CVE-2023-35363, CVE-2023-35362, CVE-2023-35358, CVE-2023-35356, CVE-2023-32044, CVE-2023-32038, CVE-2023-35365, CVE-2023-35361, CVE-2023-35360, CVE-2023-35298, CVE-2023-35296, CVE-2023-32085, CVE-2023-32083, CVE-2023-32057, CVE-2023-32056, CVE-2023-33169, CVE-2023-36874, CVE-2023-35357, CVE-2023-32050, CVE-2023-33168, CVE-2023-35364, CVE-2023-32037, CVE-2023-35348, CVE-2023-35353, CVE-2023-35352, CVE-2023-35351, CVE-2023-35350, CVE-2023-35347, CVE-2023-35343, CVE-2023-35342, CVE-2023-35341, CVE-2023-35340, CVE-2023-35339, CVE-2023-35338, CVE-2023-35337, CVE-2023-35336, CVE-2023-35332, CVE-2023-35331, CVE-2023-35330, CVE-2023-35329, CVE-2023-35328, CVE-2023-35326, CVE-2023-35325, CVE-2023-35324, CVE-2023-35323, CVE-2023-35322, CVE-2023-35321, CVE-2023-35320, CVE-2023-35319, CVE-2023-35318, CVE-2023-35317, CVE-2023-35316, CVE-2023-35315, CVE-2023-35314, CVE-2023-35313, CVE-2023-35312, CVE-2023-35300, CVE-2023-35297, CVE-2023-32084, CVE-2023-32049, CVE-2023-32046, CVE-2023-32045, CVE-2023-32043, CVE-2023-32042, CVE-2023-32041, CVE-2023-32040, CVE-2023-32039, |

| | |
|---|---|
| | CVE-2023-32035, CVE-2023-32034, CVE-2023-32033, CVE-2023-33173, CVE-2023-33172, CVE-2023-33167, CVE-2023-33166, CVE-2023-33164, CVE-2023-33163, CVE-2023-29347, CVE-2023-21756 |
| Vendor Reference: | KB5028166, KB5028168, KB5028169, KB5028171, KB5028182, KB5028185, KB5028186, KB5028222, KB5028223, KB5028224, KB5028226, KB5028228, KB5028232, KB5028233, KB5028240 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - July 2023
The KB Articles associated with the update:
The patch version for KB5028228 (https://support.microsoft.com/en-in/help/5028228)6.3.9600.21074
The patch version for KB5028223 (https://support.microsoft.com/en-in/help/5028223)6.3.9600.21074
The patch version for KB5028222 (https://support.microsoft.com/en-in/help/5028222)6.0.6003.22174
The patch version for KB5028226 (https://support.microsoft.com/en-in/help/5028226)6.0.6003.22174
The patch version for KB5028169 (https://support.microsoft.com/en-in/help/5028169)10.0.14393.6085
The patch version for KB5028168 (https://support.microsoft.com/en-in/help/5028168)10.0.17763.4644
The patch version for KB5028171 (https://support.microsoft.com/en-in/help/5028171)10.0.20348.1850
The patch version for KB5028186 (https://support.microsoft.com/en-in/help/5028186)10.0.10240.20048
The patch version for KB5028166 (https://support.microsoft.com/en-in/help/5028166)10.0.19041.3208
The patch version for KB5028185 (https://support.microsoft.com/en-in/help/5028185)10.0.22621.1992
The patch version for KB5028182 (https://support.microsoft.com/en-in/help/5028182)10.0.22000.2176
The patch version for KB5028232 (https://support.microsoft.com/en-in/help/5028232)6.2.9200.24374
The patch version for KB5028233 (https://support.microsoft.com/en-in/help/5028233)6.2.9200.24374
The patch version for KB5028240 (https://support.microsoft.com/en-in/help/5028240)6.1.7601.26623
The patch version for KB5028224 (https://support.microsoft.com/en-in/help/5028224)6.1.7601.26623

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5028228 (https://support.microsoft.com/en-in/help/5028228)
KB5028223 (https://support.microsoft.com/en-in/help/5028223)
KB5028222 (https://support.microsoft.com/en-in/help/5028222)
KB5028226 (https://support.microsoft.com/en-in/help/5028226)
KB5028169 (https://support.microsoft.com/en-in/help/5028169)
KB5028168 (https://support.microsoft.com/en-in/help/5028168)
KB5028171 (https://support.microsoft.com/en-in/help/5028171)
KB5028186 (https://support.microsoft.com/en-in/help/5028186)
KB5028166 (https://support.microsoft.com/en-in/help/5028166)
KB5028185 (https://support.microsoft.com/en-in/help/5028185)
KB5028182 (https://support.microsoft.com/en-in/help/5028182)
KB5028232 (https://support.microsoft.com/en-in/help/5028232)
KB5028233 (https://support.microsoft.com/en-in/help/5028233)
KB5028240 (https://support.microsoft.com/en-in/help/5028240)
KB5028224 (https://support.microsoft.com/en-in/help/5028224)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5028228 (https://support.microsoft.com/en-in/help/5028228)
KB5028223 (https://support.microsoft.com/en-in/help/5028223)
KB5028222 (https://support.microsoft.com/en-in/help/5028222)
KB5028226 (https://support.microsoft.com/en-in/help/5028226)
KB5028169 (https://support.microsoft.com/en-in/help/5028169)
KB5028168 (https://support.microsoft.com/en-in/help/5028168)
KB5028171 (https://support.microsoft.com/en-in/help/5028171)
KB5028186 (https://support.microsoft.com/en-in/help/5028186)
KB5028166 (https://support.microsoft.com/en-in/help/5028166)
KB5028185 (https://support.microsoft.com/en-in/help/5028185)
KB5028182 (https://support.microsoft.com/en-in/help/5028182)
KB5028232 (https://support.microsoft.com/en-in/help/5028232)
KB5028233 (https://support.microsoft.com/en-in/help/5028233)
KB5028240 (https://support.microsoft.com/en-in/help/5028240)
KB5028224 (https://support.microsoft.com/en-in/help/5028224)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2023-35356
Description: Microsoft Windows Kernel Arbitrary Read
Link: https://packetstormsecurity.com/files/174115/Microsoft-Windows-Kernel-Arbitrary-Read.html

Reference: CVE-2023-35356
Description: Microsoft Windows Kernel Security Descriptor Use-After-Free
Link: https://packetstormsecurity.com/files/174118/Microsoft-Windows-Kernel-Security-Descriptor-Use-After-Free.html

Reference: CVE-2023-35357
Description: Microsoft Windows Kernel Unsafe Reference
Link: https://packetstormsecurity.com/files/174116/Microsoft-Windows-Kernel-Unsafe-Reference.html

Reference: CVE-2023-35358
Description: Microsoft Windows Kernel Unsafe Reference
Link: https://packetstormsecurity.com/files/174117/Microsoft-Windows-Kernel-Unsafe-Reference.html

Reference: CVE-2023-36874
Description: Microsoft Error Reporting Local Privilege Elevation
Link: https://packetstormsecurity.com/files/174843/Microsoft-Error-Reporting-Local-Privilege-Elevation.html

metasploit

Reference: CVE-2023-36874
Description: Microsoft Error Reporting Local Privilege Elevation Vulnerability
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/local/win_error_cve_2023_36874.rb

cisa-alerts

Reference: CVE-2023-36874
Description: CISA Adds Five Known Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/07/11/cisa-adds-five-known-vulnerabilities-catalog

Reference: CVE-2023-32046
Description: CISA Adds Five Known Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/07/11/cisa-adds-five-known-vulnerabilities-catalog

Reference: CVE-2023-32049
Description: CISA Adds Five Known Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/07/11/cisa-adds-five-known-vulnerabilities-catalog

0day.today

Reference: CVE-2023-36874
Description: Microsoft Error Reporting Local Privilege Elevation Exploit
Link: https://0day.today/exploit/39081

github-exploits

Reference: CVE-2023-36874
Description: Wh04m1001/CVE-2023-36874 exploit repository
Link: https://github.com/Wh04m1001/CVE-2023-36874

Reference: CVE-2023-36874
Description: crisprss/CVE-2023-36874 exploit repository
Link: https://github.com/crisprss/CVE-2023-36874

Reference: CVE-2023-36874
Description: c4m3l-security/CVE-2023-36874 exploit repository
Link: https://github.com/c4m3l-security/CVE-2023-36874

Reference: CVE-2023-36874
Description: Octoberfest7/CVE-2023-36874_BOF exploit repository
Link: https://github.com/Octoberfest7/CVE-2023-36874_BOF

coreimpact

Reference: CVE-2023-36874
Description: Windows Error Reporting Local Privilege Escalation Exploit BOF
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev

Reference: CVE-2023-36874
Description: Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2023-32046
Description: Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2023-32049
Description: Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

gitlab-exploits

Reference: CVE-2023-36874
Description: Adrien_CHAMUSSY/cve-2023-36874 exploit repository
Link: https://gitlab.com/Adrien_CHAMUSSY/cve-2023-36874

google-0day-itw

Reference: CVE-2023-32046
Description: Microsoft Windows MSHTML Platform Elevation of Privilege
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2023-36874
Description: Microsoft Windows Windows Error Reporting Service Elevation of Privilege
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2023-36874
Description: The Cyberthreat Report
Link: https://www.trellix.com/advanced-research-center/threat-reports/november-2023/

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2023-36874
Type: Exploit
Platform: Win64

RESULTS:

KB5028166 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

4 Microsoft Windows Search Remote Code Execution (RCE) Vulnerability

| | |
|---|---|
| QID: | 92038 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-36884 |
| Vendor Reference: | CVE-2023-36884 |
| Bugtraq ID: | - |
| Service Modified: | 11/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft released updates to fix Windows Search remote code execution vulnerability.
The patch version is 6.3.9600.21501 for 5029312 (https://support.microsoft.com/en-in/help/5029312)
The patch version is 6.3.9600.21501 for 5029304 (https://support.microsoft.com/en-in/help/5029304)
The patch version is 6.2.9200.24412 for 5029295 (https://support.microsoft.com/en-in/help/5029295)
The patch version is 6.2.9200.24412 for 5029308 (https://support.microsoft.com/en-in/help/5029308)
The patch version is 6.1.7601.26662 for 5029296 (https://support.microsoft.com/en-in/help/5029296)
The patch version is 6.1.7601.26662 for 5029307 (https://support.microsoft.com/en-in/help/5029307)
The patch version is 6.0.6003.22214 for 5029318 (https://support.microsoft.com/en-in/help/5029318)
The patch version is 6.0.6003.22214 for 5029301 (https://support.microsoft.com/en-in/help/5029301)
The patch version is 10.0.14393.6167 for 5029242 (https://support.microsoft.com/en-in/help/5029242)
The patch version is 10.0.10240.20107 for 5029259 (https://support.microsoft.com/en-in/help/5029259)
The patch version is 10.0.19041.3324 for 5029244 (https://support.microsoft.com/en-in/help/5029244)
The patch version is 10.0.22621.2134 for 5029263 (https://support.microsoft.com/en-in/help/5029263)
The patch version is 10.0.22000.2295 for 5029253 (https://support.microsoft.com/en-in/help/5029253)
The patch version is 10.0.20348.1906 for 5029250 (https://support.microsoft.com/en-in/help/5029250)
The patch version is 10.0.17763.4737 for 5029247 (https://support.microsoft.com/en-in/help/5029247)

IMPACT:

Successful exploitation allows attacker to send the targeted user a specially crafted file that is designed to exploit the remote code execution vulnerability.

SOLUTION:

Please refer to the following KB Articles associated with the update:
5029312 (https://support.microsoft.com/en-in/help/5029312)
5029304 (https://support.microsoft.com/en-in/help/5029304)
5029295 (https://support.microsoft.com/en-in/help/5029295)
5029308 (https://support.microsoft.com/en-in/help/5029308)
5029296 (https://support.microsoft.com/en-in/help/5029296)
5029307 (https://support.microsoft.com/en-in/help/5029307)
5029318 (https://support.microsoft.com/en-in/help/5029318)
5029301 (https://support.microsoft.com/en-in/help/5029301)
5029242 (https://support.microsoft.com/en-in/help/5029242)
5029259 (https://support.microsoft.com/en-in/help/5029259)
5029244 (https://support.microsoft.com/en-in/help/5029244)
5029263 (https://support.microsoft.com/en-in/help/5029263)
5029253 (https://support.microsoft.com/en-in/help/5029253)
5029250 (https://support.microsoft.com/en-in/help/5029250)
5029247 (https://support.microsoft.com/en-in/help/5029247)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5029242 (https://support.microsoft.com/en-in/help/5029242)
KB5029244 (https://support.microsoft.com/en-in/help/5029244)
KB5029247 (https://support.microsoft.com/en-in/help/5029247)
KB5029250 (https://support.microsoft.com/en-in/help/5029250)
KB5029253 (https://support.microsoft.com/en-in/help/5029253)
KB5029259 (https://support.microsoft.com/en-in/help/5029259)
KB5029263 (https://support.microsoft.com/en-in/help/5029263)
KB5029295 (https://support.microsoft.com/en-in/help/5029295)
KB5029296 (https://support.microsoft.com/en-in/help/5029296)
KB5029301 (https://support.microsoft.com/en-in/help/5029301)
KB5029304 (https://support.microsoft.com/en-in/help/5029304)
KB5029307 (https://support.microsoft.com/en-in/help/5029307)
KB5029308 (https://support.microsoft.com/en-in/help/5029308)
KB5029312 (https://support.microsoft.com/en-in/help/5029312)
KB5029318 (https://support.microsoft.com/en-in/help/5029318)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

cisa-alerts
Reference: CVE-2023-36884
Description: CISA Adds One Known Exploited Vulnerability to Catalog
Link: https://cisa.gov/news-events/alerts/2023/07/17/cisa-adds-one-known-exploited-vulnerability-catalog

github-exploits
Reference: CVE-2023-36884
Description: jakabakos/CVE-2023-36884-MS-Office-HTML-RCE exploit repository
Link: https://github.com/jakabakos/CVE-2023-36884-MS-Office-HTML-RCE

cisa-kev

Reference: CVE-2023-36884
Description: Microsoft Office and Windows HTML Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2023-36884
Description: Microsoft Windows Office and Windows HTML Remote Code Execution
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs
Reference: CVE-2023-36884
Description: In-Depth Analysis of July 2023 Exploit Chain Featuring CVE-2023-36884 and CVE-2023-36584
Link: https://unit42.paloaltonetworks.com/new-cve-2023-36584-discovered-in-attack-chain-used-by-russian-apt/

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2023-36884
Type: Exploit
Platform: Shortcut,Document,Email,Win32,Script

Malware ID: CVE-2017-0199
Type: Exploit
Platform: Document

Qualys Cloud Threat DB
Malware ID: Underground
Type: Ransomware
Link: https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

RESULTS:

KB5029244 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

4 Microsoft Windows Security Update for September 2023

| | |
|---|---|
| QID: | 92057 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-36803, CVE-2023-38142, CVE-2023-38160, CVE-2023-38161, CVE-2023-36801, CVE-2023-36802, CVE-2023-36804, CVE-2023-36805, CVE-2023-38139, CVE-2023-38140, CVE-2023-38141, CVE-2023-38143, CVE-2023-38144, CVE-2023-38146, CVE-2023-38147, CVE-2023-38148, CVE-2023-38149, CVE-2023-38150, CVE-2023-38152, CVE-2023-38162, CVE-2023-35355 |
| Vendor Reference: | KB5030209, KB5030211, KB5030213, KB5030214, KB5030216, KB5030217, KB5030219, KB5030220, KB5030261, KB5030265, KB5030269, KB5030271, KB5030278, KB5030279, KB5030286, KB5030287, KB5030325 |
| Bugtraq ID: | - |
| Service Modified: | 12/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows Security Update - September 2023
The Patch Version is 10.0.14393.62525030213 (https://support.microsoft.com/en-in/help/5030213)
The Patch Version is 10.0.19041.34485030211 (https://support.microsoft.com/en-in/help/5030211)
The Patch Version is 10.0.22621.22835030219 (https://support.microsoft.com/en-in/help/5030219)
The Patch Version is 10.0.22000.24165030217 (https://support.microsoft.com/en-in/help/5030217)
The Patch Version is 10.0.20348.19705030216 (https://support.microsoft.com/en-in/help/5030216)
The Patch Version is 10.0.17763.48515030214 (https://support.microsoft.com/en-in/help/5030214)
The Patch Version is 6.3.9600.215635030269 (https://support.microsoft.com/en-in/help/5030269)

The Patch Version is 6.3.9600.215635030287 (https://support.microsoft.com/en-in/help/5030287)
The Patch Version is 6.2.9200.244625030278 (https://support.microsoft.com/en-in/help/5030278)
The Patch Version is 6.2.9200.244625030279 (https://support.microsoft.com/en-in/help/5030279)
The Patch Version is 6.1.7601.267135030265 (https://support.microsoft.com/en-in/help/5030265)
The Patch Version is 6.1.7601.267135030261 (https://support.microsoft.com/en-in/help/5030261)
The Patch Version is 6.0.6003.222645030271 (https://support.microsoft.com/en-in/help/5030271)
The Patch Version is 6.0.6003.222645030286 (https://support.microsoft.com/en-in/help/5030286)
The Patch Version is 10.0.10240.201615030220 (https://support.microsoft.com/en-in/help/5030220)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
5030213 (https://support.microsoft.com/en-in/help/5030213)
5030211 (https://support.microsoft.com/en-in/help/5030211)
5030219 (https://support.microsoft.com/en-in/help/5030219)
5030217 (https://support.microsoft.com/en-in/help/5030217)
5030216 (https://support.microsoft.com/en-in/help/5030216)
5030214 (https://support.microsoft.com/en-in/help/5030214)
5030269 (https://support.microsoft.com/en-in/help/5030269)
5030287 (https://support.microsoft.com/en-in/help/5030287)
5030278 (https://support.microsoft.com/en-in/help/5030278)
5030279 (https://support.microsoft.com/en-in/help/5030279)
5030265 (https://support.microsoft.com/en-in/help/5030265)
5030261 (https://support.microsoft.com/en-in/help/5030261)
5030271 (https://support.microsoft.com/en-in/help/5030271)
5030286 (https://support.microsoft.com/en-in/help/5030286)
5030220 (https://support.microsoft.com/en-in/help/5030220)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
KB5030213 (https://support.microsoft.com/en-in/help/5030213)
KB5030211 (https://support.microsoft.com/en-in/help/5030211)
KB5030219 (https://support.microsoft.com/en-in/help/5030219)
KB5030217 (https://support.microsoft.com/en-in/help/5030217)
KB5030216 (https://support.microsoft.com/en-in/help/5030216)
KB5030214 (https://support.microsoft.com/en-in/help/5030214)
KB5030269 (https://support.microsoft.com/en-in/help/5030269)
KB5030287 (https://support.microsoft.com/en-in/help/5030287)
KB5030278 (https://support.microsoft.com/en-in/help/5030278)
KB5030279 (https://support.microsoft.com/en-in/help/5030279)
KB5030265 (https://support.microsoft.com/en-in/help/5030265)
KB5030261 (https://support.microsoft.com/en-in/help/5030261)
KB5030271 (https://support.microsoft.com/en-in/help/5030271)
KB5030286 (https://support.microsoft.com/en-in/help/5030286)
KB5030220 (https://support.microsoft.com/en-in/help/5030220)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2023-36803
Description: Microsoft Windows Kernel Out-Of-Bounds Reads / Memory Disclosure
Link: https://packetstormsecurity.com/files/175109/Microsoft-Windows-Kernel-Out-Of-Bounds-Reads-Memory-Disclosure.html

Reference: CVE-2023-38139
Description: Microsoft Windows Kernel Refcount Overflow / Use-After-Free
Link: https://packetstormsecurity.com/files/174849/Microsoft-Windows-Kernel-Refcount-Overflow-Use-After-Free.html

Reference: CVE-2023-38140
Description: Microsoft Windows Kernel Paged Pool Memory Disclosure
Link: https://packetstormsecurity.com/files/175108/Microsoft-Windows-Kernel-Paged-Pool-Memory-Disclosure.html

Reference: CVE-2023-38141
Description: Microsoft Windows Kernel Race Condition / Memory Corruption
Link: https://packetstormsecurity.com/files/175096/Microsoft-Windows-Kernel-Race-Condition-Memory-Corruption.html

cisa-alerts

Reference: CVE-2023-36802
Description:

CISA Adds Two Known Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/09/12/cisa-adds-two-known-vulnerabilities-catalog

github-exploits
Reference: CVE-2023-38146
Description: Jnnshschl/CVE-2023-38146 exploit repository
Link: https://github.com/Jnnshschl/CVE-2023-38146

Reference: CVE-2023-36802
Description: x0rb3l/CVE-2023-36802-MSKSSRV-LPE exploit repository
Link: https://github.com/x0rb3l/CVE-2023-36802-MSKSSRV-LPE

Reference: CVE-2023-36802
Description: 4zur-0312/CVE-2023-36802 exploit repository
Link: https://github.com/4zur-0312/CVE-2023-36802

Reference: CVE-2023-36802
Description: chompie1337/Windows_MSKSSRV_LPE_CVE-2023-36802 exploit repository
Link: https://github.com/chompie1337/Windows_MSKSSRV_LPE_CVE-2023-36802

Reference: CVE-2023-38146
Description: gabe-k/themebleed exploit repository
Link: https://github.com/gabe-k/themebleed

Reference: CVE-2023-36802
Description: Nero22k/cve-2023-36802 exploit repository
Link: https://github.com/Nero22k/cve-2023-36802

Reference: CVE-2023-38146
Description: Durge5/ThemeBleedPy exploit repository
Link: https://github.com/Durge5/ThemeBleedPy

coreimpact
Reference: CVE-2023-36802
Description: Microsoft Streaming Service Elevation of Privilege Vulnerability Exploit (CVE-2023-36802)
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev
Reference: CVE-2023-36802
Description: Microsoft Streaming Service Proxy Privilege Escalation Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2023-36802
Description: Microsoft Windows Streaming service proxy elevation of privilege
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs
Reference: CVE-2023-36802
Description: CVE-2023-36802: Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
Link: https://googleprojectzero.github.io/0days-in-the-wild/0day-RCAs/2023/CVE-2023-36802.html

Reference: CVE-2023-36802
Description: Critically close to zero(day): Exploiting Microsoft Kernel streaming service
Link: https://securityintelligence.com/x-force/critically-close-to-zero-day-exploiting-microsoft-kernel-streaming-service/

Reference: CVE-2023-38146
Description: CVE-2023-38146: Arbitrary Code Execution via Windows Themes
Link: https://exploits.forsale/themebleed/

ASSOCIATED MALWARE:
ReversingLabs

| | |
|---|---|
| Malware ID: | CVE-2023-38146 |
| Type: | Exploit |
| Platform: | Win32,Win64,Script |

RESULTS:

KB5030211 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.19041.2965

4 Microsoft HTTP/2 Protocol Distributed Denial of Service (DoS) Vulnerability

| | |
|---|---|
| QID: | 92067 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-44487 |
| Vendor Reference: | Microsoft Security Advisory |
| Bugtraq ID: | - |
| Service Modified: | 12/14/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

CVE-2023-44487: The HTTP/2 protocol is vulnerable to Distributed Denial of Service (DDoS) attack also known as 'HTTP/2 Rapid Reset' attack. This allows malicious actors to launch a DDoS attack targeting HTTP/2 servers.
Affected Products:
Windows Server 2019
Windows Server 2016
Windows Server 2022
Windows 11 Version 21H2
Windows 11 Version 22H2
Windows 10 Version 21H2
Windows 10 Version 22H2
Windows 10 Version 1607
Microsoft Windows 10 Version 1809
.NET 7.0 and 6.0
ASP.NET Core 7.0 and 6.0
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.6
Microsoft Visual Studio 2022 version 17.7

IMPACT:

Successful exploitation of this vulnerability may allow an attacker targeting HTTP/2 servers to consume server resource significantly leads to denial of service.

SOLUTION:

Customers are advised to refer to Microsoft Security Advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487) for more information pertaining to this vulnerability.Workaround:Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave either of these workarounds in place:
1. Disable the HTTP/2 protocol on your web server by using the Registry Editor
2. Include a protocols setting for each Kestral endpoint to limit your application to HTTP1.1
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

cisa-alerts

| | |
|---|---|
| Reference: | CVE-2023-44487 |
| Description: | CISA Adds Five Known Vulnerabilities to Catalog |
| Link: | https://cisa.gov/news-events/alerts/2023/10/10/cisa-adds-five-known-vulnerabilities-catalog |

github-exploits

Reference: CVE-2023-44487
Description: pabloec20/rapidreset exploit repository
Link: https://github.com/pabloec20/rapidreset

Reference: CVE-2023-44487
Description: studiogangster/CVE-2023-44487 exploit repository
Link: https://github.com/studiogangster/CVE-2023-44487

Reference: CVE-2023-44487
Description: ReToCode/golang-CVE-2023-44487 exploit repository
Link: https://github.com/ReToCode/golang-CVE-2023-44487

Reference: CVE-2023-44487
Description: imabee101/CVE-2023-44487 exploit repository
Link: https://github.com/imabee101/CVE-2023-44487

Reference: CVE-2023-44487
Description: bcdannyboy/CVE-2023-44487 exploit repository
Link: https://github.com/bcdannyboy/CVE-2023-44487

Reference: CVE-2023-44487
Description: secengjeff/rapidresetclient exploit repository
Link: https://github.com/secengjeff/rapidresetclient

Reference: CVE-2023-44487
Description: ByteHackr/CVE-2023-44487 exploit repository
Link: https://github.com/ByteHackr/CVE-2023-44487

Reference: CVE-2023-44487
Description: nxenon/cve-2023-44487 exploit repository
Link: https://github.com/nxenon/cve-2023-44487

Reference: CVE-2023-44487
Description: ndrscodes/http2-rst-stream-attacker exploit repository
Link: https://github.com/ndrscodes/http2-rst-stream-attacker

Reference: CVE-2023-44487
Description: terrorist/HTTP-2-Rapid-Reset-Client exploit repository
Link: https://github.com/terrorist/HTTP-2-Rapid-Reset-Client

Reference: CVE-2023-44487
Description: sigridou/CVE-2023-44487- exploit repository
Link: https://github.com/sigridou/CVE-2023-44487-

cisa-kev
Reference: CVE-2023-44487
Description: HTTP/2 Rapid Reset Attack Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

nist-nvd2
Reference: CVE-2023-44487
Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
Link: https://github.com/micrictor/http2-rst-stream

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5031356 is not installed
%windir%\system32\drivers\http.sys Version is 10.0.19041.2728

4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2015-46 to MFSA 2015-58)

| | |
|---|---|
| QID: | 115070 |
| Category: | Local |
| Associated CVEs: | CVE-2015-2708, CVE-2015-2709, CVE-2015-0797, CVE-2015-2710, CVE-2015-2711, CVE-2015-2712, CVE-2015-2713, CVE-2015-2714, CVE-2015-2715, CVE-2015-2716, CVE-2015-2717, CVE-2015-2718, CVE-2011-3079, CVE-2015-2720, CVE-2015-0833 |
| Vendor Reference: | MFSA 2015-46,MFSA 2015-58 |
| Bugtraq ID: | 72747,74615,74611,53309 |
| Service Modified: | 10/30/2019 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 38
Mozilla Firefox ESR versions prior to 31.7
Mozilla Thunderbird versions prior to 31.7

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, disclose sensitive information, gain elevated privileges, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

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  1.7.0.0

4 Mozilla Firefox Diffie-Hellman Weak Encryption Vulnerability (Logjam) ((MFSA 2015-59 to MFSA 2015-71)

| | |
|---|---|
| QID: | 115167 |
| Category: | Local |
| Associated CVEs: | CVE-2015-2724, CVE-2015-2725, CVE-2015-2726, CVE-2015-2727, CVE-2015-2728, CVE-2015-2729, CVE-2015-2731, CVE-2015-2730, CVE-2015-2722, CVE-2015-2733, CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740, CVE-2015-2741, CVE-2015-2742, CVE-2015-2743, CVE-2015-4000, CVE-2015-2721 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-59 to MFSA 2015-71 |
| Bugtraq ID: | 74733,91787,75541,83398,83399 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Diffie-Hellman is a popular cryptographic algorithm used in many web browsers.
Several weaknesses in Diffie-Hellman key exchange has been found. The attack allows a man-in-the-middle to downgrade security of connections to a lower level of encryption -- 512 bit -- which can be read and attacked with relative ease.

IMPACT:

Successful exploitation of these vulnerabilities could allow attackers to affect confidentiality and integrity.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2015-2721
Description: Mozilla Network Security Services (NSS) before 3.19, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, Thunderbird before 38.1, and other products, does not properly determine state transitions for the TLS state machine, which allows man-in-the-middle attackers to defeat cryptographic protection mechanisms by blocking messages, as demonstrated by removing a forward-secrecy property by blocking a ServerKeyExchange message, aka a "SMACK SKIP-TLS" issue.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1086145

metasploit

Reference: CVE-2015-4000
Description: SSL/TLS Version Detection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/ssl/ssl_version.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities October 2007 (MFSA 2007-28 - MFSA 2007-36)

| | |
|---|---|
| QID: | 115649 |
| Category: | Local |
| Associated CVEs: | CVE-2007-1095, CVE-2007-2292, CVE-2007-4841, CVE-2007-5334, CVE-2007-5338, CVE-2007-5339, CVE-2007-5340, CVE-2007-3511, CVE-2006-2894, CVE-2007-5337 |
| Vendor Reference: | Mozilla Security |
| Bugtraq ID: | 26132,25543,24725,23668,22688,18308 |
| Service Modified: | 05/27/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation released Security update (October 19, 2007) for Firefox, SeaMonkey and Thunderbird. This update fixes a wide variety of security issues with impact ratings from Low to Critical.
MFSA 2007-36 (http://www.mozilla.org/security/announce/2007/mfsa2007-17.html) URIs with invalid %-encoding mishandled by Windows

MFSA 2007-35 (http://www.mozilla.org/security/announce/2007/mfsa2007-16.html) XPCNativeWrapper pollution using Script object

MFSA 2007-34 (http://www.mozilla.org/security/announce/2007/mfsa2007-15.html) Possible file stealing through sftp protocol

MFSA 2007-33 (http://www.mozilla.org/security/announce/2007/mfsa2007-14.html) XUL pages can hide the window title bar

MFSA 2007-32 (http://www.mozilla.org/security/announce/2007/mfsa2007-13.html) File input focus stealing vulnerability

MFSA 2007-31 (http://www.mozilla.org/security/announce/2007/mfsa2007-12.html) Browser digest authentication request splitting

MFSA 2007-30 (http://www.mozilla.org/security/announce/2007/mfsa2007-12.html) onUnload Tailgating

MFSA 2007-29 (http://www.mozilla.org/security/announce/2007/mfsa2007-12.html) Crashes with evidence of memory corruption

MFSA 2007-28 (http://www.mozilla.org/security/announce/2007/mfsa2007-12.html) Code execution via QuickTime Media-link files
These applications are affected: Mozilla Firefox2 Versions 2.0.0.7 and earlier, SeaMonkey Versions 1.1.4 and earlier, and Thunderbird2 Versions 2.0.0.7 and earlier.

IMPACT:

A remote attacker can bypass certain security restrictions and potentially compromise a vulnerable system.

SOLUTION:

Mozilla has released the following versions which fix these issues. Upgrade to the fixed or latest version as indicated below:
Firefox2 Version 2.0.0.8 (http://www.mozilla.com/firefox/) or later

Thunderbird2 Version 2.0.0.8 (http://www.mozilla.com/thunderbird/) or later

SeaMonkey Version 1.1.5 (http://www.mozilla.org/projects/seamonkey/) or later
Mozilla Foundation recommends that customers upgrade to the latest supported version of Mozilla products in order to obtain patches.
Firefox Version 1.0 and Thunderbird Version 1.0 are no longer supported. The last updates of these applications, Firefox Version 1.0.8 and Thunderbird Version 1.0.8, are affected by several vulnerabilities that are fixed in newer versions.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.8&os=win&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.8&os=linux&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.8&os=osx&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Windows (Thunderbird)
(http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-2.0.0.9&os=win&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Linux (Thunderbird)
(http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-2.0.0.9&os=linux&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Mac OS X (Thunderbird)
(http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-2.0.0.9&os=osx&lang=en-US)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Windows (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.5/seamonkey-1.1.5.en-US.win32.installer.exe)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Linux (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.5/seamonkey-1.1.5.en-US.linux-i686.installer.tar.gz)
MFSA 2007-28,MFSA 2007-29,MFSA 2007-30,MFSA 2007-31,MFSA 2007-32,MFSA 2007-33,MFSA 2007-34,MFSA 2007-35,MFSA 2007-36: Mac OS X (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.5/seamonkey-1.1.5.en-US.mac.dmg)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2006-2894
Description: Microsoft Internet Explorer 5.5/6.0/7.0 - JavaScript Key Filtering - The Exploit-DB Ref : 27986
Link: http://www.exploit-db.com/exploits/27986

Reference: CVE-2006-2894
Description: Mozilla Firefox 1.x - JavaScript Key Filtering - The Exploit-DB Ref : 27987
Link: http://www.exploit-db.com/exploits/27987

exploitdb

Reference: CVE-2006-2894
Description: Mozilla Firefox 1.x - JavaScript Key Filtering
Link: https://www.exploit-db.com/exploits/27987

Reference: CVE-2006-2894
Description: Microsoft Internet Explorer 5.5/6.0/7.0 - JavaScript Key Filtering
Link: https://www.exploit-db.com/exploits/27986

nvd

Reference: CVE-2006-2894

Description: Mozilla Firefox 1.5.0.4, 2.0.x before 2.0.0.8, Mozilla Suite 1.7.13, Mozilla SeaMonkey 1.0.2 and other versions before 1.1.5, and Netscape 8.1 and earlier allow user-assisted remote attackers to read arbitrary files by tricking a user into typing the characters of the target filename in a text box and using the OnKeyDown, OnKeyPress, and OnKeyUp Javascript keystroke events to change the focus and cause those characters to be inserted into a file upload input control, which can then upload the fi

Link: http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/046610.html

Reference: CVE-2007-3511

Description: The focus handling for the onkeydown event in Mozilla Firefox 1.5.0.12, 2.0.0.4 and other versions before 2.0.0.8, and SeaMonkey before 1.1.5 allows remote attackers to change field focus and copy keystrokes via the "for" attribute in a label, which bypasses the focus prevention, as demonstrated by changing focus from a textarea to a file upload field.

Link: http://yathong.googlepages.com/FirefoxFocusBug.html

seebug

Reference: CVE-2006-2894

Description: Internet Explorer 5.5/6.0/7.0 JavaScript Key Filtering Vulnerability

Link: https://www.seebug.org/vuldb/ssvid-81570

Reference: CVE-2006-2894

Description: Firefox 1.x JavaScript Key Filtering Vulnerability

Link: https://www.seebug.org/vuldb/ssvid-81571

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox, SeaMonkey Multiple Vulnerabilities November 2007 (MFSA 2007-37 - MFSA 2007-39)

| | |
|---|---|
| QID: | 115668 |
| Category: | Local |
| Associated CVEs: | CVE-2007-5960, CVE-2007-5959, CVE-2007-5947 |
| Vendor Reference: | RHSA-2007:1082, Mozilla Security |
| Bugtraq ID: | 26593,26589,26385 |
| Service Modified: | 08/03/2022 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation released Security update (November 26, 2007) for Firefox and SeaMonkey. This update fixes a wide variety of security issues with impact ratings of High.
MFSA 2007-39 (http://www.mozilla.org/security/announce/2007/mfsa2007-39.html) Referer-spoofing via window.location race condition

MFSA 2007-38 (http://www.mozilla.org/security/announce/2007/mfsa2007-38.html) Memory corruption vulnerabilities

MFSA 2007-37 (http://www.mozilla.org/security/announce/2007/mfsa2007-37.html) jar: URI scheme cross-site scripting hazard

These applications are affected: Mozilla Firefox2 Versions 2.0.0.9 and earlier, and SeaMonkey Versions 1.1.5 and earlier.

IMPACT:

A remote attacker can bypass certain security restrictions and potentially compromise a vulnerable system.

SOLUTION:

Mozilla has released the following versions which fix these issues. Upgrade to the fixed or latest version as indicated below:
Firefox2 Version 2.0.0.10 (http://www.mozilla.com/firefox/) or later

SeaMonkey Version 1.1.6 (http://www.mozilla.org/projects/seamonkey/) or later
Mozilla Foundation recommends that customers upgrade to the latest supported version of Mozilla products in order to obtain patches.
Red Hat users please refer to Red Hat security advisory RHSA-2007:1082 (http://rhn.redhat.com/errata/RHSA-2007-1082.html) for patches and further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.10&os=win&lang=en-US)
MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.10&os=linux&lang=en-US)
MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-2.0.0.10&os=osx&lang=en-US)
MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Windows (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.7/seamonkey-1.1.7.en-US.win32.installer.exe)
MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Linux (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.7/seamonkey-1.1.7.en-US.linux-i686.installer.tar.gz)
MFSA 2007-37,MFSA 2007-38,MFSA 2007-39: Mac OS X (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.7/seamonkey-1.1.7.en-US.mac.dmg)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 4 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities February 2008 Security Update (MFSA 2008-01 through MFSA 2008-10)

| | |
|---|---|
| QID: | 115710 |
| Category: | Local |
| Associated CVEs: | CVE-2008-0412, CVE-2008-0413, CVE-2008-0414, CVE-2008-0415, CVE-2008-0419, CVE-2008-0591, CVE-2008-0593, CVE-2008-0417, CVE-2008-0418, CVE-2008-0420, CVE-2008-0592 |
| Vendor Reference: | Mozilla Security |
| Bugtraq ID: | 27683,24293 |
| Service Modified: | 05/27/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation released a Security Update (February 2008) for Firefox, SeaMonkey and Thunderbird. This update fixes a wide variety of security issues with impact ratings from Low to Critical.

MFSA 2008-01 (http://www.mozilla.org/security/announce/2008/mfsa2008-01.html)
- Memory corruption leading to a crash
MFSA 2008-02 (http://www.mozilla.org/security/announce/2008/mfsa2008-02.html) - Multiple file input
focus stealing vulnerabilities
MFSA 2008-03 (http://www.mozilla.org/security/announce/2008/mfsa2008-03.html) - Privilege escalation, XSS,
Remote Code Execution
MFSA 2008-05 (http://www.mozilla.org/security/announce/2008/mfsa2008-05.html) - Directory traversal via chrome:
URI
MFSA 2008-06 (http://www.mozilla.org/security/announce/2008/mfsa2008-06.html) - Web browsing history and forward navigation
stealing
MFSA 2008-08 (http://www.mozilla.org/security/announce/2008/mfsa2008-08.html) - File action dialog tampering
MFSA 2008-10
(http://www.mozilla.org/security/announce/2008/mfsa2008-10.html) - URL token stealing via stylesheet redirect

The following applications
are affected:

Firefox2 Versions 2.0.0.11 and earlier
Thunderbird2 Versions 2.0.0.11 and earlier
SeaMonkey Versions 1.1.7 and
earlier

IMPACT:

As a result, a remote attacker can bypass certain security restrictions and potentially compromise a vulnerable system.

SOLUTION:

The Mozilla Foundation recommends that customers upgrade to the latest supported version of Mozilla products in order to obtain patches. Mozilla has released the following versions to address these issues. Upgrade to the fixed version shown below or a later version:

Firefox2 Version 2.0.0.12 (http://www.mozilla.com/firefox/)
Thunderbird2 Version 2.0.0.12 (http://www.mozilla.com/thunderbird/)
SeaMonkey Version 1.1.8 (http://www.mozilla.org/projects/seamonkey/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2008-01 (http://www.mozilla.org/security/announce/2008/mfsa2008-01.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2008-0418
Description: Mozilla Firefox 2.0 - 'chrome://' URI JavaScript File Request Information Disclosure - The Exploit-DB Ref : 31051
Link: http://www.exploit-db.com/exploits/31051

exploitdb

Reference: CVE-2008-0418
Description: Mozilla Firefox 2.0 - 'chrome://' URI JavaScript File Request Information Disclosure
Link: https://www.exploit-db.com/exploits/31051

nvd

Reference: CVE-2008-0591
Description: Mozilla Firefox before 2.0.0.12 and Thunderbird before 2.0.0.12 does not properly manage a delay timer used in confirmation dialogs, which might allow remote attackers to trick users into confirming an unsafe action, such as remote file execution, by using a timer to change the window focus, aka the "dialog refocus bug" or "ffclick2".
Link: http://lcamtuf.coredump.cx/ffclick2/

Reference: CVE-2008-0592
Description: Mozilla Firefox before 2.0.0.12 and SeaMonkey before 1.1.8 allows user-assisted remote attackers to cause a denial of service via a plain .txt file with a "Content-Disposition: attachment" and an invalid "Content-Type: plain/text," which prevents Firefox from rendering future plain text files within the browser.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=387258

seebug

Reference: CVE-2008-0418
Description: Mozilla Firefox 2.0 chrome:// URI JavaScript File Request Information Disclosure Vulnerability
Link: https://www.seebug.org/vuldb/ssvid-84404

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox URI Splitting Security Bypass Vulnerability

| | |
|---|---|
| QID: | 115860 |
| Category: | Local |
| Associated CVEs: | CVE-2008-2933 |
| Vendor Reference: | MFSA2008-35 |
| Bugtraq ID: | 30242 |
| Service Modified: | 03/28/2013 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

A security bypass vulnerability exists in Mozilla Firefox due to a design error.

IMPACT:

Successful exploitation would enable a remote attacker to bypass certain security restrictions and launch restricted URIs.

SOLUTION:

Upgrade to the latest version of Mozilla Firefox (http://www.mozilla.com/en-US/firefox/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2008-35 (http://www.mozilla.org/security/announce/2008/mfsa2008-35.html)

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  Version is  0.8.0.0

### 4 Mozilla Firefox and SeaMonkey Multiple Vulnerabilities

| | |
|---|---|
| QID: | 115963 |
| Category: | Local |
| Associated CVEs: | CVE-2008-0016, CVE-2008-3835, CVE-2008-3837, CVE-2008-4058, CVE-2008-4059, CVE-2008-4060, CVE-2008-4061, CVE-2008-4062, CVE-2008-4063, CVE-2008-4064, CVE-2008-4065, CVE-2008-4066, CVE-2008-4067, CVE-2008-4068, CVE-2008-4069, CVE-2008-4070, CVE-2008-3836 |
| Vendor Reference: | MFSA2008-37, MFSA2008-38, MFSA2008-40, MFSA2008-41, MFSA2008-42, MFSA2008-43, MFSA2008-44, MFSA2008-45, MFSA2008-46 |
| Bugtraq ID: | 31397,31411,31346 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Multiple vulnerabilities exists within Mozilla Firefox and SeaMonkey.

IMPACT:

Successful exploitation of these vulnerabilities may allow execution of arbitrary code.

SOLUTION:

Upgrade to the latest version of Mozilla Firefox (http://www.mozilla.com/firefox/).
Upgrade to the latest version of SeaMonkey (http://www.seamonkey-project.org/).
Refer to Red Hat Firefox advisory RHSA-2008-0879 (https://rhn.redhat.com/errata/RHSA-2008-0879.html) for patches and further details.
Refer to Red Hat Seamonkey advisory RHSA-2008-0882 (https://rhn.redhat.com/errata/RHSA-2008-0882.html) for patches and further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2008-37 (https://www.mozilla.org/en-US/security/advisories/mfsa2008-37/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security
Reference: CVE-2008-0016

Description: Mozilla Firefox UTF-8 Buffer Overflow Exploit - Core Security Category : Exploits/Client Side

Immunity

Reference: CVE-2008-0016
Description: firefox_utf8 - Immunity Ref : firefox_utf8
Link: http://immunityinc.com

The Exploit-DB

Reference: CVE-2008-0016
Description: Mozilla Firefox 2.0.0.16 - UTF-8 URL Remote Buffer Overflow - The Exploit-DB Ref : 9663
Link: http://www.exploit-db.com/exploits/9663

exploitdb

Reference: CVE-2008-0016
Description: Mozilla Firefox 2.0.0.16 - UTF-8 URL Remote Buffer Overflow
Link: https://www.exploit-db.com/exploits/9663

nvd

Reference: CVE-2008-4065
Description: Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via byte order mark (BOM) characters that are removed from JavaScript code before execution, aka "Stripped BOM characters bug."
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=430740

Reference: CVE-2008-4070
Description: Heap-based buffer overflow in Mozilla Thunderbird before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long header in a news article, related to "canceling [a] newsgroup message" and "cancelled newsgroup messages."
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=425152

Reference: CVE-2008-4067
Description: Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 on Linux allows remote attackers to read arbitrary files via a .. (dot dot) and URL-encoded / (slash) characters in a resource: URI.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=394075

Reference: CVE-2008-4067
Description: Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 on Linux allows remote attackers to read arbitrary files via a .. (dot dot) and URL-encoded / (slash) characters in a resource: URI.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=380994

Reference: CVE-2008-4066
Description: Mozilla Firefox 2.0.0.14, and other versions before 2.0.0.17, allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via HTML-escaped low surrogate characters that are ignored by the HTML parser, as demonstrated by a "jav&#56325ascript" sequence, aka "HTML escaped low surrogates bug."
Link: http://www.thespanner.co.uk/2008/06/30/javascript-protocol-fuzz-results/

Reference: CVE-2008-4066
Description: Mozilla Firefox 2.0.0.14, and other versions before 2.0.0.17, allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via HTML-escaped low surrogate characters that are ignored by the HTML parser, as demonstrated by a "jav&#56325ascript" sequence, aka "HTML escaped low surrogates bug."
Link: http://blogs.technet.com/bluehat/archive/2008/08/14/targeted-fuzzing.aspx

saint

Reference: CVE-2008-0016
Description: Mozilla Firefox UTF-8 URL buffer overflow
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_utf8

canvas

Reference: CVE-2008-0016
Description: firefox_utf8
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/firefox_utf8

coreimpact

Reference: CVE-2008-0016

Description: Mozilla Firefox UTF-8 Buffer Overflow Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 0.8.0.0

4 Mozilla Firefox, Seamonkey and Thunderbird Multiple Vulnerabilities

| | |
|---|---|
| QID: | 116044 |
| Category: | Local |
| Associated CVEs: | CVE-2008-0017, CVE-2008-5015, CVE-2008-5016, CVE-2008-5017, CVE-2008-5018, CVE-2008-5019, CVE-2008-5021, CVE-2008-5022, CVE-2008-5023, CVE-2008-5024, CVE-2008-5012, CVE-2008-5014, CVE-2008-4582, CVE-2008-5013 |
| Vendor Reference: | MFSA2008-47, MFSA2008-48, MFSA2008-49, MFSA2008-50, MFSA2008-51, MFSA2008-52, MFSA2008-53, MFSA2008-54, MFSA2008-55, MFSA2008-56, MFSA2008-57, MFSA2008-58 |
| Bugtraq ID: | 32281,31747,31611,32351 |
| Service Modified: | 08/03/2022 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Multiple vulnerabilities exists within Mozilla Firefox:
1) An error when processing "file:" URIs can be exploited to execute
arbitrary JavaScript code with chrome privileges by tricking a user into opening a malicious local file in a tab previously opened for a "chrome:" document or a privileged "about:" URI.
2) Various errors in the layout engine can be exploited to cause memory
corruption and potentially execute arbitrary code.
3) An error in the browser engine can be exploited to cause a crash.
4) An error in
the JavaScript engine can be exploited to cause a memory corruption and potentially execute arbitrary code.
5) An error in the browser's
restore feature can be exploited to violate the same-origin policy.
6) An error in the processing of the "http-index-format" MIME
type can be exploited to execute arbitrary code.
7) An error in the DOM constructing code can be exploited to dereference uninitialized
memory and potentially execute arbitrary code.
8) An error in "nsXMLHttpRequest::NotifyEventListeners()" can be exploited to
bypass certain security restrictions.
9) An error can be exploited to manipulate signed JAR files and execute arbitrary JavaScript code in
the context of another site.
10) An error exists when parsing E4X documents can be exploited to inject arbitrary XML code.

IMPACT:

These vulnerabilities can be exploited by malicious people to disclose sensitive information, bypass certain security restrictions, or compromise a user's system.

SOLUTION:

Upgrade to the latest version of Mozilla Firefox (http://www.mozilla.com/firefox/).
Upgrade to the latest version of SeaMonkey (http://www.seamonkey-project.org/).

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 Version is 0.8.0.0

4 Mozilla Firefox 3.0.5/2.0.0.19 Not Installed/Multiple Vulnerabilities (MFSA 2008-69)

| | |
|---|---|
| QID: | 116089 |
| Category: | Local |
| Associated CVEs: | CVE-2008-5513, CVE-2008-5512, CVE-2008-5511, CVE-2008-5510, CVE-2008-5508, CVE-2008-5507, CVE-2008-5506, CVE-2008-5505, CVE-2008-5504, CVE-2008-5503, CVE-2008-5502, CVE-2008-5501, CVE-2008-5500 |
| Vendor Reference: | Firefox 3.0.5 |
| Bugtraq ID: | 32878,32882 |
| Service Modified: | 12/19/2008 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
Multiple vulnerabilities exist in Firefox versions prior to versions 2.0.0.19 and 3.0.5:
1) Multiple errors in the layout engine can be exploited to corrupt memory and potentially execute arbitrary code.
2) An error in the processing of XBL bindings can be exploited to bypass the same-origin policy and read data from a target document in another domain. Successful exploitation of this vulnerability requires that the target document contains a "bindingsi" element and that the "id" of the read binding is known.
3) An error in the feed preview functionality can be exploited to execute arbitrary JavaScript code with chrome privileges.
4) An error exists when processing "XMLHttpRequest" requests to a Web server which redirects the browser via a 302 HTTP status code. This can be exploited to bypass the same-origin policy and disclose sensitive information from another domain.
5) An error exists when processing JavaScript URLs redirecting the browser to another domain returning non-JavaScript data. This can be exploited to disclose sensitive information from the other domain via a "window.onerror" event handler.
6) An error when processing URLs starting with whitespace or certain control characters can be exploited to output a malformed URL when rendering a hyperlink.
7) An error in the CSS parser when processing '\ 0'sequences can be exploited to potentially bypass third party script sanitation routines.
8) An error when processing an XBL binding attached to an unloaded document can be exploited to bypass the same-origin policy and execute arbitrary JavaScript code in a different domain.
9) Two errors can be exploited to pollute "XPCNativeWrappers" and execute arbitrary JavaScript code with chrome privileges.
10) Several errors in the session restore feature can be exploited to execute arbitrary JavaScript code in a different domain or with chrome privileges.

IMPACT:

Successful exploitation by remote attackers could lead to denial of service, cross-site scripting, information disclosure, privilege escalation and/or execution of arbitrary code.

SOLUTION:

Upgrade to the latest version of Mozilla Firefox (http://www.mozilla.com/firefox/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox 3.0.5/2.0.0.19: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.2&os=linux&lang=en-US)
Mozilla Firefox 3.0.5/2.0.0.19: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.2&os=osx&lang=en-US)
Mozilla Firefox 3.0.5/2.0.0.19: Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.2&os=win&lang=en-US)

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 Version is 0.8.0.0

4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities (MFSA 2009-01 to -06 RHSA-2009:0256 RHSA-2009:0257)

| | |
|---|---|
| QID: | 116184 |
| Category: | Local |
| Associated CVEs: | CVE-2009-0352, CVE-2009-0353, CVE-2009-0354, CVE-2009-0355, CVE-2009-0356, CVE-2009-0357, CVE-2009-0358 |
| Vendor Reference: | SUSE-SA-2009-009, RHSA-2009:0256, RHSA-2009:0257, MFSA 2009-01, MFSA 2009-02, MFSA 2009-03, MFSA 2009-04, MFSA 2009-05, MFSA 2009-06 |

| | |
|---|---|
| Bugtraq ID: | 33598 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. Thunderbird is a standalone mail and newsgroup client. SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The following security vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
1) Multiple memory corruption vulnerabilities exist in the JavaScript engines and layout engines. These exploits can cause the application to crash or cause arbitrary code execution. These issues affect Firefox, Thunderbird, and SeaMonkey. (CVE-2009-0352 and CVE-2009-0353)
2) A vulnerability in Firefox 3.x releases can be exploited to violate the same origin policy. The problem occurs in the chrome XBL method when used in conjunction with "window.eval". An attacker can exploit this issue to execute JavaScript in the context of another website. (CVE-2009-0354)
3) An information disclosure vulnerability in Firefox allows the form input control type of a closed tab to be changed when it is re-opened. An attacker can trick an unsuspecting user into re-opening a specific closed-tab to change the input type to "file" and run scripts to steal the contents of the user's local file, which may help in further attacks. (CVE-2009-0355)
4) A privilege escalation vulnerability exists due to a fix for an earlier vulnerability (MFSA 2008-47). If an attacker can trick a user into using a specific ".desktop" shortcut file to open a malicious HTML file locally, the attacker may be able to execute arbitrary code with chrome privileges. This issue affects Firefox and SeaMonkey. (CVE-2009-0356)
5) A security bypass vulnerability occurs because cookies marked "HTTPOnly" are readable by JavaScript through the "XMLHttpRequest.getResponseHeader" and "XMLHttpRequest.getAllResponseHeaders" APIs. An attacker can exploit this vulnerability to bypass the "HTTPOnly" flag security restrictions to gain access to "document.cookie". This issue affects Firefox and SeaMonkey. (CVE-2009-0357)
6) An information disclosure vulnerability occurs because the "Cache-Control: no-store" and "Cache-Control: no-cache" HTTP directives are being ignored by Firefox. This results in potentially sensitive information being stored by the browser, allowing other local users access to the cached data. Information obtained may aid in further attacks. (CVE-2009-0358)

IMPACT:

If these vulnerabilities are successfully exploited, it can cause the application to crash or cause arbitrary code execution with elevated privileges. Successful exploitation may also allow unauthorized disclosure of information which can aid in further attacks.

SOLUTION:

Workaround:
CVE-2009-0352, CVE-2009-0353: Disable JavaScript until a version containing the fixes is installed.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.6&os=win&lang=en-US)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.6&os=linux&lang=en-US)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.6&os=osx&lang=en-US)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Windows (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.15/seamonkey-1.1.15.en-US.win32.stub-installer.exe)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Linux (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.15/seamonkey-1.1.15.en-US.linux-i686.stub-installer.tar.gz)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Mac OS X (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.15/seamonkey-1.1.15.en-US.mac.dmg)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Windows (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=win&lang=en-US)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Linux (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=linux&lang=en-US)
MFSA 2009-01 to -06 RHSA-2009-0256 RHSA-2009-0257: Mac OS X (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=osx&lang=en-US)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-1.9.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/i386/xulrunner-devel-1.9.0.6-1.el5.i386.rpm?__gda__=1274832083_e82fb2a3cab346ba8012fa62c78fe3a7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (nss-pkcs11-devel-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/i386/nss-pkcs11-devel-3.12.2.0-4.el5.i386.rpm?__gda__=1274832083_a3c5f034b6e344d581472ec0e06ab130&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-unstable-1.9.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.6-1.el5/i386/xulrunner-devel-unstable-1.9.0.6-1.el5.i386.rpm?__gda__=1274832084_d166fe57c5dc1008390763438edc0f3e&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (nss-tools-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-4.el5/i386/nss-tools-3.12.2.0-4.el5.i386.rpm?__gda__=1274832084_d13090786e4c93031521af69a2f807d9&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (nss-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/i386/nss-3.12.2.0-4.el5.i386.rpm?__gda__=1274832085_22f104823da2aa5176f3244ae77c34c5&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (firefox-3.0.6-1.el5.i386)

(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el5/i386/firefox-3.0.6-1.el5.i386.rpm?__gda__=1274832085_6694e3f74bf7278d2ddfd3a0c6a6903e&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-1.9.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/i386/xulrunner-1.9.0.6-1.el5.i386.rpm?__gda__=1274832086_0235145cc85e72087a89e4eb9f862e47&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (nss-devel-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/i386/nss-devel-3.12.2.0-4.el5.i386.rpm?__gda__=1274832086_4c72ef179403b6a6c091912db1be2e11&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.6-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/ppc/xulrunner-devel-1.9.0.6-1.el5.ppc.rpm?__gda__=1274832087_219b9e3945a3c5417fcbf46daedf8f34&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-devel-3.12.2.0-4.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/ppc64/nss-devel-3.12.2.0-4.el5.ppc64.rpm?__gda__=1274832087_4b9c161214fabb03414a497d9c91bf31&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-3.12.2.0-4.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/ppc64/nss-3.12.2.0-4.el5.ppc64.rpm?__gda__=1274832088_62990d25004e5ba4d7457eb10ac643c6&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (firefox-3.0.6-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el5/ppc/firefox-3.0.6-1.el5.ppc.rpm?__gda__=1274832088_1e0a4488cd7a12911a4be17dc572a8d4&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-unstable-1.9.0.6-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.6-1.el5/ppc/xulrunner-devel-unstable-1.9.0.6-1.el5.ppc.rpm?__gda__=1274832089_7c8c6fa67ef10c00eb74b23b28f62dec&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.6-1.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/ppc64/xulrunner-1.9.0.6-1.el5.ppc64.rpm?__gda__=1274832089_0632462780bd01b9ed4480cedd71efd6&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-devel-3.12.2.0-4.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/ppc/nss-devel-3.12.2.0-4.el5.ppc.rpm?__gda__=1274832090_e6fd2ed9a1d99f21d17b47d4268b329b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-tools-3.12.2.0-4.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-4.el5/ppc/nss-tools-3.12.2.0-4.el5.ppc.rpm?__gda__=1274832090_4b18f89e0ee98481a3f9892899e07d46&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-pkcs11-devel-3.12.2.0-4.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/ppc/nss-pkcs11-devel-3.12.2.0-4.el5.ppc.rpm?__gda__=1274832091_1a8d5cf697bdb224bfc9b4d565ee3454&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.6-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/ppc/xulrunner-1.9.0.6-1.el5.ppc.rpm?__gda__=1274832091_a56214861325502473b152887a535245&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-3.12.2.0-4.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/ppc/nss-3.12.2.0-4.el5.ppc.rpm?__gda__=1274832092_5fcd92061981d497cd25abc01e2177ee&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (nss-pkcs11-devel-3.12.2.0-4.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/ppc64/nss-pkcs11-devel-3.12.2.0-4.el5.ppc64.rpm?__gda__=1274832092_db217c3351c169dd1ebde72c44d61c56&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.6-1.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/ppc64/xulrunner-devel-1.9.0.6-1.el5.ppc64.rpm?__gda__=1274832093_b0eff963f4264feb838b233c064ff5d3&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (nss-devel-3.12.2.0-4.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/ia64/nss-devel-3.12.2.0-4.el5.ia64.rpm?__gda__=1274832093_1126e995d1c90598c4b28ac0bbb2ae4b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-1.9.0.6-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/ia64/xulrunner-1.9.0.6-1.el5.ia64.rpm?__gda__=1274832094_fc2b244bd7c44da46809e8df8ffcbade&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (nss-tools-3.12.2.0-4.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-4.el5/ia64/nss-tools-3.12.2.0-4.el5.ia64.rpm?__gda__=1274832094_2f7ab9eeecaabeedb00b46baa1a833d5&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (firefox-3.0.6-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el5/ia64/firefox-3.0.6-1.el5.ia64.rpm?__gda__=1274832095_dc0c2dbb89192d07a4239aefb524de8a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (nss-pkcs11-devel-3.12.2.0-4.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/ia64/nss-pkcs11-devel-3.12.2.0-4.el5.ia64.rpm?__gda__=1274832095_cae3ef16eee78da02ca84bebfdbfec4b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (nss-3.12.2.0-4.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/ia64/nss-3.12.2.0-4.el5.ia64.rpm?__gda__=1274832096_62b883c3c4bc5e9c6d1b8f7b29f67c48&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-1.9.0.6-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/ia64/xulrunner-devel-1.9.0.6-1.el5.ia64.rpm?__gda__=1274832096_8c97aff34d6e2a2453574351553f7a5a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (nss-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/i386/nss-3.12.2.0-4.el5.i386.rpm?__gda__=1274832097_cd487b835285eb96a27e00cf457deadc&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-unstable-1.9.0.6-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.6-1.el5/ia64/xulrunner-devel-unstable-1.9.0.6-1.el5.ia64.rpm?__gda__=1274832097_3763e23f4fa0c019d4e59464a6787aa6&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-3.12.2.0-4.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/x86_64/nss-3.12.2.0-4.el5.x86_64.rpm?__gda__=1274832098_a2e688e329b276b7c537ac5b8780a01b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-pkcs11-devel-3.12.2.0-4.el5.x86_64)

(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/x86_64/nss-pkcs11-devel-3.12.2.0-4.el5.x86_64.rpm?__gda__=1274832098_1a06f6148c12dbc4217bd661efdaec89&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.6-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/x86_64/xulrunner-1.9.0.6-1.el5.x86_64.rpm?__gda__=1274832100_d5b34c235998ae408e1a53b8a64d22a2&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/i386/xulrunner-devel-1.9.0.6-1.el5.i386.rpm?__gda__=1274832101_b0c2b7b39dbc584657b83f8fc702d39a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-unstable-1.9.0.6-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.6-1.el5/x86_64/xulrunner-devel-unstable-1.9.0.6-1.el5.x86_64.rpm?__gda__=1274832101_8dd7482f78707d5d63654e5b426a5fc1&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-tools-3.12.2.0-4.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-4.el5/x86_64/nss-tools-3.12.2.0-4.el5.x86_64.rpm?__gda__=1274832102_919a995d4277265686f1ac279d4313b4&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-pkcs11-devel-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-pkcs11-devel/3.12.2.0-4.el5/i386/nss-pkcs11-devel-3.12.2.0-4.el5.i386.rpm?__gda__=1274832102_a1f4ef44ad314bfffe5b72f7c402dfc7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-devel-3.12.2.0-4.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/x86_64/nss-devel-3.12.2.0-4.el5.x86_64.rpm?__gda__=1274832103_8dc2dd555881e26787a5e5c728283aa9&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (firefox-3.0.6-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el5/x86_64/firefox-3.0.6-1.el5.x86_64.rpm?__gda__=1274832103_dda51e5c59b6f5c20bf5bb4c0e1b2ba5&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-4.el5/i386/nss-3.12.2.0-4.el5.i386.rpm?__gda__=1274832104_6349ba1ec420057357c2b234284ea448&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (firefox-3.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el5/i386/firefox-3.0.6-1.el5.i386.rpm?__gda__=1274832104_ac0bd434112ca43fc57708226542232a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.6-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.6-1.el5/i386/xulrunner-1.9.0.6-1.el5.i386.rpm?__gda__=1274832105_543c677a67680753f7ed1aeb03dc2efb&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (nss-devel-3.12.2.0-4.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-4.el5/i386/nss-devel-3.12.2.0-4.el5.i386.rpm?__gda__=1274832105_126cfae3b69d49d188a007d34badd1c0&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.6-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.6-1.el5/x86_64/xulrunner-devel-1.9.0.6-1.el5.x86_64.rpm?__gda__=1274832106_5f192e19896247c363ac07d451de4e95&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (firefox-3.0.6-1.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/i386/firefox-3.0.6-1.el4.i386.rpm?__gda__=1274832106_16179911601b14a4b6c683fd8338c6fd&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (nss-tools-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/i386/nss-tools-3.12.2.0-3.el4.i386.rpm?__gda__=1274832107_045426e7d74c2a0d8a2051217f11ff53&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (nss-devel-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/i386/nss-devel-3.12.2.0-3.el4.i386.rpm?__gda__=1274832107_7c4612762f6394f794b932cf42e351b7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832108_e7495f20f1bb2daf3b5519e59c36bd4b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (nss-tools-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/x86_64/nss-tools-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832108_57cfca0e3cec02bbc9f71c532bd9b279&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (firefox-3.0.6-1.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/x86_64/firefox-3.0.6-1.el4.x86_64.rpm?__gda__=1274832109_47a372b52b840942630e1a3275ce10e4&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (nss-devel-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/x86_64/nss-devel-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832109_b99fa14b780e675ae63cdc0161c75d88&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (nss-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/x86_64/nss-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832110_8bbedd3e1e57e065e14adce12895862b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832111_834ce9927b8860ac6a7130964a113a67&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (firefox-3.0.6-1.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/ppc/firefox-3.0.6-1.el4.ppc.rpm?__gda__=1274832111_43ca8629ff6698ee68e34e233274cc1d&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (nss-3.12.2.0-3.el4.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/ppc64/nss-3.12.2.0-3.el4.ppc64.rpm?__gda__=1274832112_704bd1457695231c430cad8c46337ffc&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (nss-3.12.2.0-3.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/ppc/nss-3.12.2.0-3.el4.ppc.rpm?__gda__=1274832112_e009785d1d66bb79c2ed6945eb068d4a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (nss-tools-3.12.2.0-3.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/ppc/nss-tools-3.12.2.0-3.el4.ppc.rpm?__gda__=1274832113_779fdc220869f0ab9a4350ada159b3f7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (nss-devel-3.12.2.0-3.el4.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/ppc/nss-devel-3.12.2.0-3.el4.ppc.rpm?__gda__=1274832113_bff33ff3d65ccfceb26cd8aa2732dbe2&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (firefox-3.0.6-1.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/ia64/firefox-3.0.6-1.el4.ia64.rpm?__gda__=1274832114_d992ac782ba16e5dabc947e377d692ae&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (nss-devel-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/ia64/nss-devel-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832114_629f8be827777b61d6c3352aaa053a4b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (nss-tools-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/ia64/nss-tools-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832115_63d48f5f7ac5c757d730825c732697f7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832115_50eb306a6295bde15947479ebce3208f&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (nss-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/ia64/nss-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832116_5ccc5374df39e07a88f5aa57f5655e0c&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (firefox-3.0.6-1.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/i386/firefox-3.0.6-1.el4.i386.rpm?__gda__=1274832116_35432121dee86638de5a64bd2f80944b&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (nss-tools-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/i386/nss-tools-3.12.2.0-3.el4.i386.rpm?__gda__=1274832117_d02268bbecf1a0057bc7d70ea0508dcd&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (nss-devel-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/i386/nss-devel-3.12.2.0-3.el4.i386.rpm?__gda__=1274832117_3cf8effa918a50e299f077afe6322949&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832118_00b235887173b7f45e625f875820d73f&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (firefox-3.0.6-1.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/ia64/firefox-3.0.6-1.el4.ia64.rpm?__gda__=1274832118_d815bed90273134fe6ebcb8f901bd5eb&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (nss-devel-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/ia64/nss-devel-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832119_8164b48420781ef9ecb2dcd52894ec64&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (nss-tools-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/ia64/nss-tools-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832119_543a1f1923b210a8b3c67277077aa46d&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832120_a81341e559152ddec237a6701b59397a&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (nss-3.12.2.0-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/ia64/nss-3.12.2.0-3.el4.ia64.rpm?__gda__=1274832120_fcb5feb89a8f10c6c164de3c9c98e8cc&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (nss-tools-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-tools/3.12.2.0-3.el4/x86_64/nss-tools-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832121_7873d7b28b51bd11453dc4c3d412cdd7&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (firefox-3.0.6-1.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.6-1.el4/x86_64/firefox-3.0.6-1.el4.x86_64.rpm?__gda__=1274832121_5b7deb7db75033b9ba74162e0f82baee&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (nss-devel-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss-devel/3.12.2.0-3.el4/x86_64/nss-devel-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832122_76e1f111d30be57dd5ac6551a0290657&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (nss-3.12.2.0-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/x86_64/nss-3.12.2.0-3.el4.x86_64.rpm?__gda__=1274832122_1441901c0bb70b4c3ddba7ca06e726e5&ext=.rpm)
RHSA-2009:0256: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (nss-3.12.2.0-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/nss/3.12.2.0-3.el4/i386/nss-3.12.2.0-3.el4.i386.rpm?__gda__=1274832123_e18f162c565f1d09f185fc09750a0b36&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/x86_64/seamonkey-nss-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832132_e6c8fc042656cde23f1c6e5ae911e5e4&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/x86_64/seamonkey-nspr-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832133_fb77d0fc24b490cd4caba37e1dd0eead&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/x86_64/seamonkey-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832133_01b392e9cf475d0d09a8d6eac3cd75d2&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/x86_64/seamonkey-nspr-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832134_703727d331b46c25985238e2c8e7c2e0&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-js-debugger-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/x86_64/seamonkey-js-debugger-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832134_302d29ce7a88c616487ed0e38a24703b&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/x86_64/seamonkey-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832135_d8b25cdc54bb09a43ceb55e59a9ef34f&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-chat-1.0.9-0.32.el3.x86_64)

(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/x86_64/seamonkey-chat-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832135_7d97c40a40ab77acaf77e957a2b613b8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/x86_64/seamonkey-nss-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832136_b3137f19a0af40070a4513c7df96efad&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-mail-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/x86_64/seamonkey-mail-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832136_91c50408b35bce51f97b7044d954a60d&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-dom-inspector-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/x86_64/seamonkey-dom-inspector-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832137_7c0b1e92e7e9fd932a41527ed75832b0&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/i386/seamonkey-1.0.9-0.32.el3.i386.rpm?__gda__=1274832137_e66a38b37d3d23c0fece388a73329ed5&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832138_7d543700536fb1224c7a9049956b68fc&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832138_ce50865d8a96e985329c232c26b17d64&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nss-devel-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/ia64/seamonkey-nss-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832139_75957b907f5c335b994a2c0ee359a234&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nss-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/ia64/seamonkey-nss-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832139_f0989c3f4c911850021deb0a525d3e18&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nspr-devel-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/ia64/seamonkey-nspr-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832140_9053bc24f4911475e17678e9d1c1a3fb&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-mail-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/ia64/seamonkey-mail-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832140_f7457cb9c9c1e162cc5ba3e898accb2a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-js-debugger-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/ia64/seamonkey-js-debugger-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832141_1d3aa0b03abce7e06c490750cc42e894&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-devel-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/ia64/seamonkey-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832141_03f37721983abe56106570cdaef10ec5&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-chat-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/ia64/seamonkey-chat-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832142_d666b700c713d061414cceb33d645e2c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nspr-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/ia64/seamonkey-nspr-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832142_ceca82d9bf01348e6a6a376e225aaf3e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-dom-inspector-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/ia64/seamonkey-dom-inspector-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832143_ce819abd4e9e6bc91e227c7fc298a713&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/ia64/seamonkey-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832143_0b2b8dd3808fe31cf497dd56793aa958&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832144_4f778210b1d87e2776091a78c0ab5cd2&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for Itanium) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832144_365657ca19f10c6988ebf6d8f231f117&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-nspr-devel-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/ppc/seamonkey-nspr-devel-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832145_d9c2d6b55b8e78a449cfb73eb5f83ecc&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/ppc/seamonkey-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832145_12c433dcd09f637acbe4c31cd0ccded7&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-js-debugger-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/ppc/seamonkey-js-debugger-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832146_be916e53b366f308176865f430fcb6e8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-nss-devel-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/ppc/seamonkey-nss-devel-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832146_9c35898b5193724d845dd5b30e5e1ec4&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-dom-inspector-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/ppc/seamonkey-dom-inspector-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832147_4ed6ae5b8d17b4d2fc37013ef7540773&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-chat-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/ppc/seamonkey-chat-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832147_c40c62c069a011d80310f774b2546d9c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-nss-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/ppc/seamonkey-nss-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832148_323ad07a6954c452fa900ea2e5dc41ac&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-mail-1.0.9-0.32.el3.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/ppc/seamonkey-mail-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832148_1227a62a2308c609ba021cd6eae3eae9&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-devel-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/ppc/seamonkey-devel-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832149_9e3bede7d8bb61f818933facfc1656d0&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for iSeries and pSeries) (seamonkey-nspr-1.0.9-0.32.el3.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/ppc/seamonkey-nspr-1.0.9-0.32.el3.ppc.rpm?__gda__=1274832149_ce34cdff4428e8ff720f157e9563352d&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-nspr-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/i386/seamonkey-nspr-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832150_1cd0e9966adb1f453f4ccdcfc9872f89&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/i386/seamonkey-1.0.9-0.32.el3.i386.rpm?__gda__=1274832150_5248ff8654272bf524369bd38e697df4&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-nss-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/i386/seamonkey-nss-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832151_a7258169ddc81c8b86573204b111ec8a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-chat-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/i386/seamonkey-chat-1.0.9-0.32.el3.i386.rpm?__gda__=1274832151_d2e6b3e13a49129dba5076415e0c9c57&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/i386/seamonkey-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832152_2320e987b229157ed8c20a6aa3ba81d3&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-mail-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/i386/seamonkey-mail-1.0.9-0.32.el3.i386.rpm?__gda__=1274832152_032891c289fa2fd5836f5a3ab3c70062&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-js-debugger-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/i386/seamonkey-js-debugger-1.0.9-0.32.el3.i386.rpm?__gda__=1274832153_abf213c8318a33d5f180cbedce70d7a8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-dom-inspector-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/i386/seamonkey-dom-inspector-1.0.9-0.32.el3.i386.rpm?__gda__=1274832153_08498aa63aba9fbe393d1604e281c302&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832154_77bfbac2cc76086d4855192a42d007f6&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 3 for x86) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832154_a22e66f36decc47071372bc988ca1d24&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-devel-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/i386/seamonkey-devel-1.0.9-35.el4.i386.rpm?__gda__=1274832155_66bcbdf413d9ca5b151d3ff79e666cd6&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-chat-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/i386/seamonkey-chat-1.0.9-35.el4.i386.rpm?__gda__=1274832155_32d009f0fa24a401d77a00158a14e42f&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-dom-inspector-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/i386/seamonkey-dom-inspector-1.0.9-35.el4.i386.rpm?__gda__=1274832156_10501ee87b0d7dbef6bc720657238751&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-js-debugger-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/i386/seamonkey-js-debugger-1.0.9-35.el4.i386.rpm?__gda__=1274832156_640d7c0e6dab3db4b1fa63ceec2479e1&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-mail-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/i386/seamonkey-mail-1.0.9-35.el4.i386.rpm?__gda__=1274832157_b395a5016c8c522229528fcf053ab14a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (seamonkey-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/i386/seamonkey-1.0.9-35.el4.i386.rpm?__gda__=1274832157_630699bbe64815baf4e397f7041d9d60&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-mail-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/x86_64/seamonkey-mail-1.0.9-35.el4.x86_64.rpm?__gda__=1274832158_1794aadbaec7c0b38de57909671f4fba&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-js-debugger-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/x86_64/seamonkey-js-debugger-1.0.9-35.el4.x86_64.rpm?__gda__=1274832158_ae2e0867190b3123d15648631eb7d110&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-chat-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/x86_64/seamonkey-chat-1.0.9-35.el4.x86_64.rpm?__gda__=1274832159_9333ec7656c037871163faa793729a59&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-devel-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/x86_64/seamonkey-devel-1.0.9-35.el4.x86_64.rpm?__gda__=1274832159_ecf76c79a88cf9a07bf10498daf3c1db&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-dom-inspector-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/x86_64/seamonkey-dom-inspector-1.0.9-35.el4.x86_64.rpm?__gda__=1274832160_bde0215dffef53b25219f09b54040fa5&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (seamonkey-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/x86_64/seamonkey-1.0.9-35.el4.x86_64.rpm?__gda__=1274832160_008f2fe7828a7b6c23df409e1d0746e2&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-js-debugger-1.0.9-35.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/ppc/seamonkey-js-debugger-1.0.9-35.el4.ppc.rpm?__gda__=1274832161_84d11eee2f6a73b40f204fa1bde1562b&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-1.0.9-35.el4.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/ppc/seamonkey-1.0.9-35.el4.ppc.rpm?__gda__=1274832161_bd9b0d3685ddc9a31975cdd2d7497cf6&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-devel-1.0.9-35.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/ppc/seamonkey-devel-1.0.9-35.el4.ppc.rpm?__gda__=1274832162_003377901aca4fc709e50fb5a3feac9a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-chat-1.0.9-35.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/ppc/seamonkey-chat-1.0.9-35.el4.ppc.rpm?__gda__=1274832162_95fdcc26f8a2f23aa646c519bb6c3790&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-dom-inspector-1.0.9-35.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/ppc/seamonkey-dom-inspector-1.0.9-35.el4.ppc.rpm?__gda__=1274832163_44e8b09b3f64070310b13a8412afd7d9&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (seamonkey-mail-1.0.9-35.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/ppc/seamonkey-mail-1.0.9-35.el4.ppc.rpm?__gda__=1274832163_89f3facf4f652f6dd2eed406ba0c9ff8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-js-debugger-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/ia64/seamonkey-js-debugger-1.0.9-35.el4.ia64.rpm?__gda__=1274832164_1eddfaf8bbb1cf2e1c7021c726d68ec8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-dom-inspector-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/ia64/seamonkey-dom-inspector-1.0.9-35.el4.ia64.rpm?__gda__=1274832164_4ec57992b2d538367304a815787308eb&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/ia64/seamonkey-1.0.9-35.el4.ia64.rpm?__gda__=1274832165_9db40f6a50d292cbd227c6381f485bbe&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-mail-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/ia64/seamonkey-mail-1.0.9-35.el4.ia64.rpm?__gda__=1274832165_0df7a3ab6c70e7777fa1bcb7ff93003b&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-devel-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/ia64/seamonkey-devel-1.0.9-35.el4.ia64.rpm?__gda__=1274832166_b42785d466791b6dab51a1b31c7609bb&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (seamonkey-chat-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/ia64/seamonkey-chat-1.0.9-35.el4.ia64.rpm?__gda__=1274832166_04f007df14d56b5af40222747d182490&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/x86_64/seamonkey-nss-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832167_1053c0398efb93cedc5d422a970f4d08&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/x86_64/seamonkey-nspr-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832167_c18bcd8dfd49f5701fa02fcadfc4618c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/x86_64/seamonkey-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832168_1002b7a4218607bbe919e72e12472f1c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/x86_64/seamonkey-nspr-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832168_22b0419672836926577e2817edf2e4b0&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-js-debugger-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/x86_64/seamonkey-js-debugger-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832169_22482bc849f5c1725a73ee6386fa1ef1&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/x86_64/seamonkey-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832169_dcbd87115531a93939fdb1570c7077a7&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-chat-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/x86_64/seamonkey-chat-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832170_2bebf315caebdbe6a7b83bdd6bc82e6f&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-devel-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/x86_64/seamonkey-nss-devel-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832170_3392e0461f38482caefe9f13b786109a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-mail-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/x86_64/seamonkey-mail-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832171_49e82cdb0b0bc054d32dbc2ade12f4f8&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-dom-inspector-1.0.9-0.32.el3.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/x86_64/seamonkey-dom-inspector-1.0.9-0.32.el3.x86_64.rpm?__gda__=1274832171_330700e09d022a755a03a2478586a925&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/i386/seamonkey-1.0.9-0.32.el3.i386.rpm?__gda__=1274832172_4524551bae0c98fde2b82f5390f85c71&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832172_21bce668ba0835d81a113e81a9178968&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for AMD64/Intel EM64T) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832173_1d91f65d7e325c13e2ea151cf954548c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nss-devel-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/ia64/seamonkey-nss-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832174_12203af65a753843a81afed7f4758b49&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nss-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/ia64/seamonkey-nss-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832174_c2887ce3acfcc8acdf9e8807f355c107&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nspr-devel-1.0.9-0.32.el3.ia64)

(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/ia64/seamonkey-nspr-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832175_4eff610ebd3c03027c375c1de3a238f3&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-mail-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/ia64/seamonkey-mail-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832175_d075a5b61aa5356695b43a03235d90ec&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-js-debugger-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/ia64/seamonkey-js-debugger-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832176_ae1aed805c9c5ecf5df081659fd99040&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-devel-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/ia64/seamonkey-devel-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832176_09712407c43f35d3d818877ff8258af5&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-chat-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/ia64/seamonkey-chat-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832176_6590a75b6c73f7a8e20b01d5b55797c3&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nspr-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/ia64/seamonkey-nspr-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832177_a49c3a3cd5fa1cbf2106f7dcbf90cf5e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-dom-inspector-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/ia64/seamonkey-dom-inspector-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832177_848e2de0e42035e6173ad658d1cce1ec&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-1.0.9-0.32.el3.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/ia64/seamonkey-1.0.9-0.32.el3.ia64.rpm?__gda__=1274832178_039bc9bccc19a66eb55e21dc9971b57d&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832179_01b1b57f226a97d8cf1b9d77b6a74e59&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for Itanium) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832179_8258bdbe61cd07cd36fce7605bf23dd3&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-nspr-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr-devel/1.0.9-0.32.el3/i386/seamonkey-nspr-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832180_3b3fe391023376e4cac835aaf4e0bb1c&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-0.32.el3/i386/seamonkey-1.0.9-0.32.el3.i386.rpm?__gda__=1274832180_32dab6b87ba33fa12f9eb8cb3ea4781a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-nss-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss-devel/1.0.9-0.32.el3/i386/seamonkey-nss-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832181_7e6102ac88c7cb752c200eae8c1cd039&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-chat-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-0.32.el3/i386/seamonkey-chat-1.0.9-0.32.el3.i386.rpm?__gda__=1274832181_9acc849e95f7b58da8fc710601256d0a&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-devel-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-0.32.el3/i386/seamonkey-devel-1.0.9-0.32.el3.i386.rpm?__gda__=1274832182_12f8cc2d23b736e53a3b4aed35fb3cae&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-mail-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-0.32.el3/i386/seamonkey-mail-1.0.9-0.32.el3.i386.rpm?__gda__=1274832182_b30fa325adf7cc8f99ceb80e8e565581&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-js-debugger-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-0.32.el3/i386/seamonkey-js-debugger-1.0.9-0.32.el3.i386.rpm?__gda__=1274832183_2a2580dbe3d8f501f96e99dea7b671ca&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-dom-inspector-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-0.32.el3/i386/seamonkey-dom-inspector-1.0.9-0.32.el3.i386.rpm?__gda__=1274832183_31514f65ecc584d0c722872651870d08&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-nss-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nss/1.0.9-0.32.el3/i386/seamonkey-nss-1.0.9-0.32.el3.i386.rpm?__gda__=1274832184_a408fef03c29c00d3cfd5736d4fd4d6e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 3 for x86) (seamonkey-nspr-1.0.9-0.32.el3.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-nspr/1.0.9-0.32.el3/i386/seamonkey-nspr-1.0.9-0.32.el3.i386.rpm?__gda__=1274832184_9a88d927ba402e8483785c6ee9999507&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-devel-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/i386/seamonkey-devel-1.0.9-35.el4.i386.rpm?__gda__=1274832185_4614e213f7c04555a91624f88a652c31&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-chat-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/i386/seamonkey-chat-1.0.9-35.el4.i386.rpm?__gda__=1274832185_1bc6d889a7f004bdff62495fe5457bce&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-dom-inspector-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/i386/seamonkey-dom-inspector-1.0.9-35.el4.i386.rpm?__gda__=1274832186_3da80218eb541af50beceaa9d3a09fc9&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-js-debugger-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/i386/seamonkey-js-debugger-1.0.9-35.el4.i386.rpm?__gda__=1274832186_38b263dcc9955dc15bee6879d1bc9d0b&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-mail-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/i386/seamonkey-mail-1.0.9-35.el4.i386.rpm?__gda__=1274832187_d434119c4f03c273c91fc54be4ba56bf&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (seamonkey-1.0.9-35.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/i386/seamonkey-1.0.9-35.el4.i386.rpm?__gda__=1274832187_27ecde2eb81368a028f6c3c8dee3f61e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-js-debugger-1.0.9-35.el4.ia64)

(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/ia64/seamonkey-js-debugger-1.0.9-35.el4.ia64.rpm?__gda__=1274832188_57a1002f885c2cd97e15f7623cac594e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-dom-inspector-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/ia64/seamonkey-dom-inspector-1.0.9-35.el4.ia64.rpm?__gda__=1274832188_9dd813217b61900005ad26a818364984&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/ia64/seamonkey-1.0.9-35.el4.ia64.rpm?__gda__=1274832189_f7e85de3771551de82c7f8b8912e3aa4&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-mail-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/ia64/seamonkey-mail-1.0.9-35.el4.ia64.rpm?__gda__=1274832189_df2a3dfdc9b92385d6bba8675ac83f8e&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-devel-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/ia64/seamonkey-devel-1.0.9-35.el4.ia64.rpm?__gda__=1274832190_453b12ddb794ea981236657b7c5607a1&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (seamonkey-chat-1.0.9-35.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/ia64/seamonkey-chat-1.0.9-35.el4.ia64.rpm?__gda__=1274832190_86c5244155242b3f7f5a3128efc90aff&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-mail-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-mail/1.0.9-35.el4/x86_64/seamonkey-mail-1.0.9-35.el4.x86_64.rpm?__gda__=1274832191_3a6735ce869668aa289fa6e9a9b8f207&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-js-debugger-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-js-debugger/1.0.9-35.el4/x86_64/seamonkey-js-debugger-1.0.9-35.el4.x86_64.rpm?__gda__=1274832191_9755e841f65b1533ca50f15bec09c3f7&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-chat-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-chat/1.0.9-35.el4/x86_64/seamonkey-chat-1.0.9-35.el4.x86_64.rpm?__gda__=1274832192_f3f05ea42aba71ea3c3497460cdfceac&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-devel-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-devel/1.0.9-35.el4/x86_64/seamonkey-devel-1.0.9-35.el4.x86_64.rpm?__gda__=1274832192_10c3272a8c34e253d27fbf141cbcbce6&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-dom-inspector-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey-dom-inspector/1.0.9-35.el4/x86_64/seamonkey-dom-inspector-1.0.9-35.el4.x86_64.rpm?__gda__=1274832193_bf672220e0cbcb28ab07fb675d31fd87&ext=.rpm)
RHSA-2009:0257: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (seamonkey-1.0.9-35.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/seamonkey/1.0.9-35.el4/x86_64/seamonkey-1.0.9-35.el4.x86_64.rpm?__gda__=1274832193_a9f11676473d23dc00409c7bb84d481a&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

ExploitKits

Reference: CVE-2009-0355
Description: Firefox - Components/sessionstore/src/nsSessionStore.js
Link: http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html

contagio

Reference: CVE-2009-0355
Description: Zero Exploit Kit
Link: https://docs.google.com/spreadsheets/d/1cK7vFVn73NTsoLU487nh-XVSFu7M064RgHeDZB0a2s8/edit#gid=0

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities (MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4)

| | |
|---|---|
| QID: | 116263 |
| Category: | Local |
| Associated CVEs: | CVE-2009-0771, CVE-2009-0772, CVE-2009-0773, CVE-2009-0774, CVE-2009-0775, CVE-2009-0776, CVE-2009-0777, CVE-2009-0040 |
| Vendor Reference: | MFSA 2009-07, MFSA 2009-08, MFSA 2009-09, MFSA 2009-10, MFSA 2009-11, RHSA-2009:0315 |
| Bugtraq ID: | 33990,33827 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |

Edited: No
PCI Vuln: Yes

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The Mozilla Foundation has released multiple advisories regarding security vulnerabilities in Firefox, Thunderbird, and SeaMonkey. The following issues have been reported:
1) Multiple memory corruption vulnerabilities affect the layout engine in Firefox, Thunderbird, and SeaMonkey. An attacker can exploit these issues to execute arbitrary code and cause the affected application to crash. (CVE-2009-0771, CVE-2009-0772, CVE-2009-0773, and CVE-2009-0774)
2) A denial of service vulnerability affecting the garbage collection service is caused due to improper memory management of a set of cloned XUL DOM elements which were linked as a parent and child. This can be exploited to cause arbitrary code execution when the browser attempts to access a destroyed object.(CVE-2009-0775)
3) A cross-domain information disclosure vulnerability affects the nsIRDFService. An attacker can exploit this issue to steal arbitrary XML data from another domain (CVE-2009-0776)
4) A vulnerability allows an attacker to spoof the location bar. The problem occurs because certain invisible control characters are being decoded, resulting in fewer visible characters being displayed in the location bar. (CVE-2009-0777)
5) Vulnerabilities in PNG libraries used by Mozilla can be exploited by to crash a browser and potentially execute arbitrary code on the user's computer via a crafted PNG file that free ups an uninitialized pointer in the "png_read_png" function, "pCAL" chunk handling, or setup of 16-bit gamma tables. (CVE-2009-0040)

IMPACT:

If these vulnerabilities are successfully exploited, it allows attackers to execute arbitrary code in the context of the browser, cause denial of service, steal arbitrary XML data from another domain and spoof the location bar to conduct phishing attacks.

SOLUTION:

Workaround:
CVE-2009-0771, CVE-2009-0772, CVE-2009-0773, CVE-2009-0774, CVE-2009-0776: Disable JavaScript until a version containing the fixes is installed.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.7&os=win&lang=en-US)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.7&os=linux&lang=en-US)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.7&os=osx&lang=en-US)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Windows (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.14/seamonkey-1.1.14.en-US.win32.stub-installer.exe)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Linux (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.14/seamonkey-1.1.14.en-US.linux-i686.stub-installer.tar.gz)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Mac OS (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.14/seamonkey-1.1.14.en-US.mac.dmg)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Windows (Thunderbird)
(www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=win&lang=en-US)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Linux (Thunderbird)
(www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=linux&lang=en-US)
MFSA 2009-07, MFSA 2009-08,MFSA 2009-09,MFSA 2009-10,MFSA 2009-11,RHSA-2009:0315-4: Mac OS (Thunderbird)
(www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=osx&lang=en-US)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-unstable-1.9.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-1.el5/i386/xulrunner-devel-unstable-1.9.0.7-1.el5.i386.rpm?__gda__=1274826433_548a3a654a255712acd27a13cd30a20e&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-1.9.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/i386/xulrunner-devel-1.9.0.7-1.el5.i386.rpm?__gda__=1274826433_b080e4d786ac1d7a4c94d7120241400d&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-1.9.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/i386/xulrunner-1.9.0.7-1.el5.i386.rpm?__gda__=1274826434_197212bfb0ae10dcc53d709a2acdfb74&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (firefox-3.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el5/i386/firefox-3.0.7-1.el5.i386.rpm?__gda__=1274826434_bfea1c18f05bdc396602984dc41eab16&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.7-1.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/ppc64/xulrunner-devel-1.9.0.7-1.el5.ppc64.rpm?__gda__=1274826435_a502929217fa07a11a12b874bab806a1&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.7-1.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/ppc64/xulrunner-1.9.0.7-1.el5.ppc64.rpm?__gda__=1274826435_85429aa51c4e27e3dc83f7cedabc1618&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-unstable-1.9.0.7-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-1.el5/ppc/xulrunner-devel-unstable-1.9.0.7-1.el5.ppc.rpm?__gda__=1274826436_0b1bb3b2d46a2306de19711903bc2f24&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.7-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/ppc/xulrunner-1.9.0.7-1.el5.ppc.rpm?__gda__=1274826436_c238d3cc9d91b5e5d9b79155a9acdedc&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (firefox-3.0.7-1.el5.ppc)

(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el5/ppc/firefox-3.0.7-1.el5.ppc.rpm?__gda__=1274826437_5e62f866d582a18c1b27aa4fd88f23b8&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.7-1.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/ppc/xulrunner-devel-1.9.0.7-1.el5.ppc.rpm?__gda__=1274826437_d54badc3bb1d61c308b152a00d1143bd&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-1.9.0.7-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/ia64/xulrunner-1.9.0.7-1.el5.ia64.rpm?__gda__=1274826438_e5fc91eb39cf1feb1e30d2614dc2ad75&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (firefox-3.0.7-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el5/ia64/firefox-3.0.7-1.el5.ia64.rpm?__gda__=1274826439_733339a051778e605a5a8cc101911b86&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-1.9.0.7-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/ia64/xulrunner-devel-1.9.0.7-1.el5.ia64.rpm?__gda__=1274826440_2fea9b50c0f04c04a4773162a8528174&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-unstable-1.9.0.7-1.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-1.el5/ia64/xulrunner-devel-unstable-1.9.0.7-1.el5.ia64.rpm?__gda__=1274826441_d5b6d095e2491b29d8c464fbbb16d4b6&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-unstable-1.9.0.7-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-1.el5/x86_64/xulrunner-devel-unstable-1.9.0.7-1.el5.x86_64.rpm?__gda__=1274826441_8372e223bf7b7b6df91c3e32dd2aa2a9&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/i386/xulrunner-devel-1.9.0.7-1.el5.i386.rpm?__gda__=1274826442_3bfcc8f98827b6058cb32a5c2fc84efc&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/i386/xulrunner-1.9.0.7-1.el5.i386.rpm?__gda__=1274826442_031947a8e583c1c3d91ebb417623494d&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.7-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-1.el5/x86_64/xulrunner-1.9.0.7-1.el5.x86_64.rpm?__gda__=1274826443_0985fd2a1de2298481f6cce679461959&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.7-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-1.el5/x86_64/xulrunner-devel-1.9.0.7-1.el5.x86_64.rpm?__gda__=1274826443_a95c505daeb119a6abf74a128fd0d457&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (firefox-3.0.7-1.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el5/i386/firefox-3.0.7-1.el5.i386.rpm?__gda__=1274826444_bf075d7ad5606174b896e6cb91432621&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (firefox-3.0.7-1.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el5/x86_64/firefox-3.0.7-1.el5.x86_64.rpm?__gda__=1274826444_9715e0cbe822eba6f8cd0621b9ffe03f&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (firefox-3.0.7-1.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/i386/firefox-3.0.7-1.el4.i386.rpm?__gda__=1274826445_6a1838fd9838bde0d42fab6f760b8a5d&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (firefox-3.0.7-1.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/x86_64/firefox-3.0.7-1.el4.x86_64.rpm?__gda__=1274826445_80f3006af16f2a7a7a8c4664ba485440&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (firefox-3.0.7-1.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/ppc/firefox-3.0.7-1.el4.ppc.rpm?__gda__=1274826446_1adc150858995b3c333aa9d6facd3e2d&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (firefox-3.0.7-1.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/ia64/firefox-3.0.7-1.el4.ia64.rpm?__gda__=1274826446_f87ef77e8500bce9c2755ae93f73ea86&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (firefox-3.0.7-1.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/i386/firefox-3.0.7-1.el4.i386.rpm?__gda__=1274826447_45bfac35c10205edd947202f3581c397&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (firefox-3.0.7-1.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/ia64/firefox-3.0.7-1.el4.ia64.rpm?__gda__=1274826447_50022ec7eedfe52ec6193aca715fbba9&ext=.rpm)
RHSA-2009:0315: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (firefox-3.0.7-1.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-1.el4/x86_64/firefox-3.0.7-1.el4.x86_64.rpm?__gda__=1274826448_6a6ac36ad3e51f14b2fff05e12a4f405&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2009-0773

Description: The JavaScript engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) a splice of an array that contains "some non-set elements," which causes jsarray.cpp to pass an incorrect argument to the ResizeSlots function, which triggers memory corruption; (2) vectors related to js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__, and watch, which triggers an

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=457521

Reference: CVE-2009-0773

Description: The JavaScript engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) a splice of an array that contains "some non-set elements," which causes jsarray.cpp to pass an incorrect argument to the ResizeSlots function, which triggers memory corruption; (2) vectors related to

js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__, and watch, which triggers an

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=467499

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Fix Two Vulnerabilities (MFSA 2009-12, MFSA 2009-13,RHSA-2009:0397)

| | |
|---|---|
| QID: | 116328 |
| Category: | Local |
| Associated CVEs: | CVE-2009-1044, CVE-2009-1169 |
| Vendor Reference: | SUSE-SA:2009:022, MFSA 2009-12, MFSA 2009-13, RHSA-2009:0397 |
| Bugtraq ID: | 34181,34235 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. The following vulnerabilities exist in in Mozilla Firefox:
1) A memory corruption and denial of service vulnerability in the "txMozillaXSLTProcessor::TransformToDoc" function in Mozilla Firefox Version 3.0.7 is caused due to the improper handling of errors encountered when transforming an XML document. This can be exploited to trigger the handling of a temporary, corrupted stack variable as an evaluation context object via specially crafted XSLT code. (CVE-2009-1169)
2) An error in the processing of the XUL tree method "_moveToEdgeShift()" can be exploited to trigger garbage collection routines on objects, which are still in use. This can cause the browser to crash when attempting to access a previously destroyed object. (CVE-2009-1044)
Mozilla Firefox Versions 3.0.7 and earlier are vulnerable.

IMPACT:

If these vulnerabilities are successfully exploited, it allows attackers to crash the browser to cause a denial of service attack or compromise a user's system. Exploitation can also result in arbitrary code execution.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Update to Firefox Version 3.0.8 available at Firefox Download site (http://www.mozilla.com/en-US/firefox/3.0.8/releasenotes/).
Refer to the Mozilla Foundation security advisories MFSA 2009-12 (http://www.mozilla.org/security/announce/2009/mfsa2009-12.html) and MFSA 2009-13 (http://www.mozilla.org/security/announce/2009/mfsa2009-13.html) for additional information.
Red Hat patches are available from the Red Hat Network (https://www.redhat.com/wapps/sso/rhn/login.html?redirect=http%3A%2F%2Frhn.redhat.com%2Frhn%2FYourRhn.do).
Steps on using the Red Hat Network (RHN) to apply packages are listed as follows:
For Red Hat Enterprise Linux Versions 2.1, 3, and 4, the interactive Update Agent can be launched with the "up2date" command.
For Red Hat Enterprise Linux Version 5, the graphical Update tool can be launched with the "pup" command.
To install packages using the command-line interface, use the command "yum update".
Refer to Red Hat security advisory RHSA-2009-0397 (https://rhn.redhat.com/errata/RHSA-2009-0397.html) to address this issue and obtain further details.
For Suse refer to security advisory SUSE-SA:2009:022 (http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00008.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-12, MFSA 2009-13,RHSA-2009-0397: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=win&lang=en-US)
MFSA 2009-12, MFSA 2009-13,RHSA-2009-0397: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=linux&lang=en-US)
MFSA 2009-12, MFSA 2009-13,RHSA-2009-0397: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=osx&lang=en-US)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-1.9.0.7-3.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/i386/xulrunner-devel-1.9.0.7-3.el5.i386.rpm?__gda__=1274829611_d17d09a569926d221823d9bf5f016acb&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-devel-unstable-1.9.0.7-3.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-3.el5/i386/xulrunner-devel-unstable-1.9.0.7-3.el5.i386.rpm?__gda__=1274829611_8ca9bea5f33d2ea23de43dda3b015e24&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 32-bit x86) (xulrunner-1.9.0.7-3.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/i386/xulrunner-1.9.0.7-3.el5.i386.rpm?__gda__=1274829612_213db09ff9f63e6aa7549a3f45d6370d&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.7-3.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/ppc/xulrunner-1.9.0.7-3.el5.ppc.rpm?__gda__=1274829612_bd1521d94b2e27fb1eeb8da

990169cdd&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.7-3.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/ppc64/xulrunner-devel-1.9.0.7-3.el5.ppc64.rpm?__gda__=1274829612_d2b3220ab40da10b6dd8ae06c4139e80&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-unstable-1.9.0.7-3.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-3.el5/ppc/xulrunner-devel-unstable-1.9.0.7-3.el5.ppc.rpm?__gda__=1274829613_2a475c00273d0c73effbce5f3b28022f&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-1.9.0.7-3.el5.ppc64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/ppc64/xulrunner-1.9.0.7-3.el5.ppc64.rpm?__gda__=1274829613_5dfe4df73dd307bf803157b32fa3e556&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit IBM POWER) (xulrunner-devel-1.9.0.7-3.el5.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/ppc/xulrunner-devel-1.9.0.7-3.el5.ppc.rpm?__gda__=1274829614_8b0dea00c5125a636efd61087644dcbc&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-unstable-1.9.0.7-3.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-3.el5/ia64/xulrunner-devel-unstable-1.9.0.7-3.el5.ia64.rpm?__gda__=1274829614_d1f4dbb6805ef8cd9ee12275fe458c59&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-1.9.0.7-3.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/ia64/xulrunner-1.9.0.7-3.el5.ia64.rpm?__gda__=1274829615_254097de5e9fad79778a05a952c61031&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit Itanium) (xulrunner-devel-1.9.0.7-3.el5.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/ia64/xulrunner-devel-1.9.0.7-3.el5.ia64.rpm?__gda__=1274829616_f37bf5bd98a4f34868d19e49fc4a252d&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-unstable-1.9.0.7-3.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel-unstable/1.9.0.7-3.el5/x86_64/xulrunner-devel-unstable-1.9.0.7-3.el5.x86_64.rpm?__gda__=1274829616_f213d1cbc2e6036f10b8236284bcb1eb&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.7-3.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/i386/xulrunner-devel-1.9.0.7-3.el5.i386.rpm?__gda__=1274829617_f51a64b07c426603443d150cf14c4abc&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.7-3.el5.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/i386/xulrunner-1.9.0.7-3.el5.i386.rpm?__gda__=1274829617_dfb9fc6e58f7ad1bfa0c8d9aa8296e41&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-1.9.0.7-3.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner/1.9.0.7-3.el5/x86_64/xulrunner-1.9.0.7-3.el5.x86_64.rpm?__gda__=1274829617_ca5cb08ce704321fb8ba5bdccd29fff8&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) (xulrunner-devel-1.9.0.7-3.el5.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/xulrunner-devel/1.9.0.7-3.el5/x86_64/xulrunner-devel-1.9.0.7-3.el5.x86_64.rpm?__gda__=1274829618_84b813ccad953eae30f40012977ba900&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) (firefox-3.0.7-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/i386/firefox-3.0.7-3.el4.i386.rpm?__gda__=1274829618_0e0269ce3eb80c5a9b94cb6f6154da4e&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T) (firefox-3.0.7-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/x86_64/firefox-3.0.7-3.el4.x86_64.rpm?__gda__=1274829619_9f2a15bef42f751b02ca02a100cd48c5&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux AS (v. 4 for 64-bit IBM POWER) (firefox-3.0.7-3.el4.ppc)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/ppc/firefox-3.0.7-3.el4.ppc.rpm?__gda__=1274829619_1f85dc718dc92676072ac839b124508c&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium) (firefox-3.0.7-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/ia64/firefox-3.0.7-3.el4.ia64.rpm?__gda__=1274829620_362d381e8442d06ada6d9c997d73be36&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) (firefox-3.0.7-3.el4.i386)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/i386/firefox-3.0.7-3.el4.i386.rpm?__gda__=1274829620_b9268dc2444e31a03877abb33cd2d21e&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux ES (v. 4 for 64-bit Intel Itanium) (firefox-3.0.7-3.el4.ia64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/ia64/firefox-3.0.7-3.el4.ia64.rpm?__gda__=1274829621_07eea27103878167afcf2f5095c6314e&ext=.rpm)
RHSA-2009:0397: Red Hat Enterprise Linux ES (v. 4 for AMD64/Intel EM64T) (firefox-3.0.7-3.el4.x86_64)
(https://content-web.rhn.redhat.com/rhn/public/NULL/firefox/3.0.7-3.el4/x86_64/firefox-3.0.7-3.el4.x86_64.rpm?__gda__=1274829621_2d9533e00061fefa385e82adcbe0cebe&ext=.rpm)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2009-1169
Description: Mozilla Firefox XSL - Parsing Remote Memory Corruption (PoC) (1) - The Exploit-DB Ref : 8285
Link: http://www.exploit-db.com/exploits/8285

exploitdb
Reference: CVE-2009-1169
Description: Mozilla Firefox XSL - Parsing Remote Memory Corruption (PoC) (1)
Link: https://www.exploit-db.com/exploits/8285

nvd
Reference: CVE-2009-1169

Description: The txMozillaXSLTProcessor::TransformToDoc function in Mozilla Firefox before 3.0.8 and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an XML file with a crafted XSLT transform.

Link: http://www.securityfocus.com/bid/34235

seebug

Reference: CVE-2009-1169

Description: Mozilla Firefox XSL - Parsing Remote Memory Corruption PoC (0day)

Link: https://www.seebug.org/vuldb/ssvid-66391

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities (MFSA 2009-14 through -22)

| | |
|---|---|
| QID: | 116385 |
| Category: | Local |
| Associated CVEs: | CVE-2009-1302, CVE-2009-1303, CVE-2009-1304, CVE-2009-1305, CVE-2009-1306, CVE-2009-1307, CVE-2009-1308, CVE-2009-1309, CVE-2009-1310, CVE-2009-1312, CVE-2009-1311, CVE-2009-0652 |
| Vendor Reference: | MFSA 2009-14, MFSA 2009-15, MFSA 2009-16, MFSA 2009-17, MFSA 2009-18, MFSA 2009-19, MFSA 2009-20, MFSA 2009-21, MFSA 2009-22 |
| Bugtraq ID: | 34656,33837 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The Mozilla Foundation has released multiple security advisories specifying various vulnerabilities in Firefox, Thunderbird and SeaMonkey. The following issues have been reported:
- Multiple errors in the browser engine and the JavaScript engine can be exploited to corrupt memory and potentially execute arbitrary code. (CVE-2009-1302, CVE-2009-1303, CVE-2009-1304, CVE-2009-1305)
- An URI-spoofing vulnerability exists because the applications fail to adequately handle specific characters in IDN subdomains. Specifically, this issue results from the display of unspecified characters resembling the '/' forward slash character. An attacker may exploit this issue to create a subdomain which visually resembles a legitimate top level domain followed by additional information. (CVE-2009-0652)
- When the jar: scheme is used to wrap a URI which serves the content with Content-Disposition: attachment, the HTTP header is ignored and the content is unpacked and displayed inline. An attacker could use this vulnerability to subvert sites using this mechanism to mitigate content injection attacks. (CVE-2009-1306)
- An error when loading a Adobe Flash file via the "view-source:" scheme can be exploited to conduct cross-site request forgery attacks or read and write Local Shared Objects on a user's system. (CVE-2009-1307)
- An error in the processing of XBL bindings on sites which allow users to embed third-party stylesheets are vulnerable to script injection attacks. (CVE-2009-1308)
- Errors in "XMLHttpRequest" and "XPCNativeWrapper.toString" can be exploited to bypass the same-origin policy and execute arbitrary JavaScript within the context of another site or execute code attacker-defined functions with chrome privileges.(CVE-2009-1309)
- A weakness exists in the handling of "SearchForm" URIs which can be exploited by an attacker by tricking a user into installing a malicious MozSearch plugin. When the user performs an empty search, the SearchForm javascript: URI would be executed within the context of the currently open page. (CVE-2009-310)
- When an inner frame of a Web page is saved as file POST data of the outer page is sent to the URL of the inner frame resulting in information disclosure. (CVE-2009-1311)
- Firefox allows "Refresh" header to redirect to javascript: URIs allowing an attacker to conduct cross-site scripting attacks. (CVE-2009-1312)

IMPACT:

Attackers can exploit these issues to bypass same-origin restrictions, obtain potentially sensitive information, and execute arbitrary script code with elevated privileges; other attacks are also possible.

SOLUTION:

Workaround:
CVE-2009-1302, CVE-2009-1303, CVE-2009-1304, CVE-2009-1305: Disable JavaScript until a version containing the fixes is installed.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2009-23: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=win&lang=en-US)
MFSA2009-23: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=linux&lang=en-US)

MFSA2009-23: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.8&os=osx&lang=en-US)
MFSA2009-23: Windows (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=win&lang=en-US)
MFSA2009-23: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=linux&lang=en-US)
MFSA2009-23: Mac OS (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.21&os=osx&lang=en-US)
MFSA2009-23: Windows (SeaMonkey) (ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.16/seamonkey-1.1.16.en-US.win32.installer.exe)
MFSA2009-23: Linux (SeaMonkey) (ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.16/seamonkey-1.1.16.en-US.linux-i686.installer.tar.gz)
MFSA2009-23: Mac OS (SeaMonkey) (ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.16/seamonkey-1.1.16.en-US.mac.dmg)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2009-1312
Description: Mozilla (Multiple Products) - Server Refresh Header Cross-Site Scripting - The Exploit-DB Ref : 32942
Link: http://www.exploit-db.com/exploits/32942

exploitdb

Reference: CVE-2009-1312
Description: Mozilla (Multiple Products) - Server Refresh Header Cross-Site Scripting
Link: https://www.exploit-db.com/exploits/32942

nvd

Reference: CVE-2009-1310
Description: Cross-site scripting (XSS) vulnerability in the MozSearch plugin implementation in Mozilla Firefox before 3.0.9 allows user-assisted remote attackers to inject arbitrary web script or HTML via a javascript: URI in the SearchForm element.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=483086

Reference: CVE-2009-1305
Description: The JavaScript engine in Mozilla Firefox before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving JSOP_DEFVAR and properties that lack the JSPROP_PERMANENT attribute.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=476049

Reference: CVE-2009-1302
Description: The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAnc
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=431260

Reference: CVE-2009-1302
Description: The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAnc
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=454276

Reference: CVE-2009-1302
Description: The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAnc
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=483444

Reference: CVE-2009-1302
Description: The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAnc
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=432114

Reference: CVE-2009-1302
Description: The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAnc
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=467881

Reference: CVE-2009-1311
Description: Mozilla Firefox before 3.0.9 and SeaMonkey before 1.1.17 allow user-assisted remote attackers to obtain sensitive information via a web page with an embedded frame, which causes POST data from an outer page to be sent to the inner frame's URL during a SAVEMODE_FILEONLY save of the inner frame.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=471962

Reference: CVE-2009-1304
Description: The JavaScript engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving (1) js_FindPropertyHelper, related to the definitions of Math and Date; and (2) js_CheckRedeclaration.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=475971

Reference: CVE-2009-1304
Description: The JavaScript engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving (1) js_FindPropertyHelper, related to the definitions of Math and Date; and (2) js_CheckRedeclaration.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=461158

Reference: CVE-2009-1308
Description: Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey allows remote attackers to inject arbitrary web script or HTML via vectors involving XBL JavaScript bindings and remote stylesheets, as exploited in the wild by a March 2009 eBay listing.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=481558

seebug
Reference: CVE-2009-1312
Description: Mozilla Multiple Products Server Refresh Header XSS
Link: https://www.seebug.org/vuldb/ssvid-86203

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: Ducky
Type: Trojan
Platform: Win32,Image

Malware ID: Mult
Type: Exploit
Platform: Script

Malware ID: IFrameBOF
Type: Exploit
Platform: Script,Document

Malware ID: ANIFile
Type: Exploit
Platform: Win32

Malware ID: LoadImage
Type: Exploit
Platform: Script

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Security Update for Firefox (MFSA2009-23)

QID: 116395
Category: Local

| | |
|---|---|
| Associated CVEs: | CVE-2009-1313 |
| Vendor Reference: | MFSA 2009-23 |
| Bugtraq ID: | 34743 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is an open source Web browser.
Firefox is prone to a remote memory corruption vulnerability that is caused due to an error when calling the "nsTextFrame::ClearTextRun()" function and can be exploited to corrupt memory. (CVE-2009-1313)
Firefox Version 3.0.9 is affected with this issue.

IMPACT:

If this vulnerability is successfully exploited, it will allow attackers to execute arbitrary code in the context of the application.
Exploitation may also cause the browser to crash, denying service to legitimate users.

SOLUTION:

The vendor has released an update (Firefox Version 3.0.10) to resolve this issue. The update is available at Mozilla Firefox Download site (http://www.mozilla.com/products/download.html?product=firefox-3.0.10&os=win&lang=en-US).
Refer to the vendor security advisory MFSA2009-23 (http://www.mozilla.org/security/announce/2009/mfsa2009-23.html) for additional information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2009-23: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.10&os=win&lang=en-US)
MFSA2009-23: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.10&os=linux&lang=en-US)
MFSA2009-23: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.10&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2009-1313
- Description: Mozilla Firefox 3.0.9 - 'nsTextFrame::ClearTextRun()' Remote Memory Corruption - The Exploit-DB Ref : 32961
- Link: http://www.exploit-db.com/exploits/32961

exploitdb
- Reference: CVE-2009-1313
- Description: Mozilla Firefox 3.0.9 - 'nsTextFrame::ClearTextRun()' Remote Memory Corruption
- Link: https://www.exploit-db.com/exploits/32961

seebug
- Reference: CVE-2009-1313
- Description: Mozilla Firefox 3.0.9 'nsTextFrame::ClearTextRun()' Remote Memory Corruption Vulnerability
- Link: https://www.seebug.org/vuldb/ssvid-86222

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Remote Vulnerabilities (MFSA 2009-24 through 2009-32)

| | |
|---|---|
| QID: | 116459 |
| Category: | Local |
| Associated CVEs: | CVE-2009-1841, CVE-2009-1840, CVE-2009-1839, CVE-2009-1838, CVE-2009-1837, CVE-2009-1836, CVE-2009-1835, CVE-2009-1834, CVE-2009-1833, CVE-2009-1832, CVE-2009-1392 |
| Vendor Reference: | MFSA 2009-24, MFSA 2009-25, MFSA 2009-26, MFSA 2009-27, MFSA 2009-28, MFSA 2009-29, MFSA 2009-30, MFSA 2009-31, MFSA 2009-32 |

| | |
|---|---|
| Bugtraq ID: | 35326,35370,35371,35372,35388,35391,35380,35360,35383,35386,35373 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The following security vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
1) Multiple unspecified memory corruption vulnerabilities affect the browser and Javascript engines. Another error could trigger double frame construction which would also lead to memory corruption. An attacker can exploit these issues to execute arbitrary code or cause crashes. This issue affects Firefox, Thunderbird and SeaMonkey. (CVE-2009-1392, CVE-2009-1832, CVE-2009-1833)
2) A URL spoofing vulnerability exists because certain invalid unicode characters, when used as part of an IDN, are displayed as whitespace in the location bar. This may allow attackers to spoof the contents and display a misleading URL for their malicious Web page. This issue affects Firefox and SeaMonkey. (CVE-2009-1834)
3) An information disclosure vulnerability affects Firefox and SeaMonkey because a local document's domain is calculated incorrectly from its URL. An attacker can exploit this issue by tricking an unsuspecting user into downloading and opening a malicious file. (CVE-2009-1835)
4) A vulnerability affects Firefox, Thunderbird, and SeaMonkey when handling a CONNECT request that is sent to a proxy server returns a non-200 response. This can cause the body of the response to be rendered in the context of the request's 'Host:' header. An attacker may be able to exploit this issue to execute arbitrary code within the victim's requested SLL-protected domain. (CVE-2009-1836)
5) A remote code execution vulnerability affects Firefox because of a race condition in 'NPObjWrapper_NewResolve' when accessing properties of a "NPObject". An attacker may be able to exploit this issue to run arbitrary code when a user navigates away from a page during the loading of a Java object because the object does not get properly destroyed. (CVE-2009-1837)
6) An arbitrary code-execution vulnerability affects Firefox, Thunderbird, and SeaMonkey because the owner document of an element can become null after garbage collection. An attacker can exploit this issue by having a malicious event handler execute arbitrary JavaScript with chrome privileges. (CVE-2009-1838)
7) A privilege escalation vulnerability affects Firefox when a 'file:' resource is loaded via the location bar. The resource inherits the principal of the previously loaded document giving the new document additional privileges to access the contents of other local files that it wouldn't otherwise have permission to read. (CVE-2009-1839)
8) A vulnerability in Firefox, Thunderbird, and SeaMonkey occurs because content-loading policies are not properly checked before loading external script files into XUL documents. (CVE-2009-1840)
9) A privilege escalation vulnerability affects Firefox and SeaMonkey because of a problem in the browser sidebar and FeedWriter. An attacker could cause a chrome privileged object to interact with Web content allowing arbitrary execution of code with the object's chrome privileges. (CVE-2009-1841)
Versions prior to Mozilla Thunderbird 2.0.0.22, Mozilla SeaMonkey 1.1.17, Mozilla Firefox 3.0.11 are vulnerable.

IMPACT:

Attackers can exploit these issues to bypass same-origin restrictions, obtain potentially sensitive information, and execute arbitrary script code with elevated privileges; other attacks are also possible.

SOLUTION:

Workaround:
For CVE-2009-1392, CVE-2009-1832, CVE-2009-1833, CVE-2009-1841: Disable JavaScript until a fixed version is installed.
For CVE-2009-1837: Disable Java until a fixed version is installed.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.11&os=win&lang=en-US)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.11&os=linux&lang=en-US)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.11&os=osx&lang=en-US)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Windows (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.17/seamonkey-1.1.17.en-US.win32.stub-installer.exe)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Linux (SeaMonkey)
(ftp://ftp.mozilla.org/pub/mozilla.org/seamonkey/releases/1.1.17/seamonkey-1.1.17.en-US.linux-i686.stub-installer.tar.gz)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Windows (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.22&os=win&lang=en-US)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Linux (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.22&os=linux&lang=en-US)
MFSA 2009-24,MFSA 2009-25,MFSA 2009-26,MFSA 2009-27,MFSA 2009-28,MFSA 2009-29,MFSA 2009-30,MFSA 2009-31,MFSA 2009-32: Mac OS (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-2.0.0.22&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


The Exploit-DB

| | |
|---|---|
| Reference: | CVE-2009-1834 |
| Description: | Mozilla Firefox 3.0.10 / SeaMonkey 1.1.16 - Address Bar URI Spoofing - The Exploit-DB Ref : 33039 |
| Link: | http://www.exploit-db.com/exploits/33039 |

Reference: CVE-2009-1839
Description: Mozilla Firefox - Location Bar Spoofing - The Exploit-DB Ref : 10544
Link: http://www.exploit-db.com/exploits/10544

exploitdb

Reference: CVE-2009-1834
Description: Mozilla Firefox 3.0.10 / SeaMonkey 1.1.16 - Address Bar URI Spoofing
Link: https://www.exploit-db.com/exploits/33039

Reference: CVE-2009-1839
Description: Mozilla Firefox - Location Bar Spoofing
Link: https://www.exploit-db.com/exploits/10544

nvd

Reference: CVE-2009-1832
Description: Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors involving "double frame construction."
Link: https://bugzilla.redhat.com/show_bug.cgi?id=503569

Reference: CVE-2009-1832
Description: Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors involving "double frame construction."
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=484031

Reference: CVE-2009-1837
Description: Race condition in the NPObjWrapper_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll in Mozilla Firefox 3 before 3.0.11 might allow remote attackers to execute arbitrary code via a page transition during Java applet loading, related to a use-after-free vulnerability for memory associated with a destroyed Java object.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=486269

Reference: CVE-2009-1833
Description: The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=426520

Reference: CVE-2009-1833
Description: The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.
Link: https://bugzilla.redhat.com/show_bug.cgi?id=503570

Reference: CVE-2009-1833
Description: The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=427196

Reference: CVE-2009-1833
Description: The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=369696

Reference: CVE-2009-1834
Description: Visual truncation vulnerability in netwerk/dns/src/nsIDNService.cpp in Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 allows remote attackers to spoof the location bar via an IDN with invalid Unicode characters that are displayed as whitespace, as demonstrated by the \u115A through \u115E characters.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=479413

Reference: CVE-2009-1836
Description: Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 use the HTTP Host header to determine the context of a document provided in a non-200 CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.
Link: https://bugzilla.redhat.com/show_bug.cgi?id=503578

Reference: CVE-2009-1836

Description: Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 use the HTTP Host header to determine the context of a document provided in a non-200 CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=479880

Reference: CVE-2009-1835

Description: Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 associate local documents with external domain names located after the file:// substring in a URL, which allows user-assisted remote attackers to read arbitrary cookies via a crafted HTML document, as demonstrated by a URL with file://example.com/C:/ at the beginning.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=491801

Reference: CVE-2009-1835

Description: Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 associate local documents with external domain names located after the file:// substring in a URL, which allows user-assisted remote attackers to read arbitrary cookies via a crafted HTML document, as demonstrated by a URL with file://example.com/C:/ at the beginning.

Link: https://bugzilla.redhat.com/show_bug.cgi?id=503576

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=486398

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=489041

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=380359

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=451341

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=490513

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.redhat.com/show_bug.cgi?id=503568

Reference: CVE-2009-1392

Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=490410

Reference: CVE-2009-1392
Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=429969

Reference: CVE-2009-1392
Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=472776

Reference: CVE-2009-1392
Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=431086

Reference: CVE-2009-1392
Description: The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventStateManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFr
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=432068

seebug
Reference: CVE-2009-1834
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-86294

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox/Thunderbird Multiple Remote Vulnerabilities (MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40)

| | |
|---|---|
| QID: | 116528 |
| Category: | Local |
| Associated CVEs: | CVE-2009-2462, CVE-2009-2463, CVE-2009-2464, CVE-2009-2465, CVE-2009-2466, CVE-2009-2467, CVE-2009-2468, CVE-2009-1194, CVE-2009-2469, CVE-2009-2471, CVE-2009-2472 |
| Vendor Reference: | MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40 |
| Bugtraq ID: | 34870,35758 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. Thunderbird is a standalone mail and newsgroup client.
The following security vulnerabilities have been identified in Firefox and Thunderbird:
- Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
- An integer overflow error in a base64 decoding function can be exploited to corrupt memory and potentially execute arbitrary code.
- An error in the handling of multiple RDF files in a XUL tree element can be exploited to corrupt memory and potentially execute arbitrary code.
- An error exists in the construction of documents, which can result in double copies of certain elements within this document.

- An error in the handling of frames can be exploited to cause a memory corruption and potentially execute arbitrary code.
- Multiple errors in the Javascript engine can be exploited to corrupt memory and potentially execute arbitrary code.
- An error in the handling of Flash objects when navigating to another page can potentially be exploited to trigger a call to a deleted object and potentially execute arbitrary code.
- Multiple vulnerabilities in various font glyph rendering libraries can be exploited by malicious people to compromise a user's system.
- An error in the handling of SVG elements on which a watch function and __defineSetter__ function have been set for a certain property can be exploited to cause a memory corruption and execute arbitrary code.
- An error when setTimeout() is invoked with certain object parameters can result in the object loosing its wrapper. This can potentially be exploited to execute arbitrary JavaScript code with chrome privileges.
- Various errors in the handling of wrappers for objects can potentially be exploited to access properties of such objects that have been set by a different site and conduct cross-site scripting attacks.

IMPACT:

If these vulnerabilities are successfully exploited, it will allow attackers to conduct cross-site scripting (XSS) attacks, execute arbitrary code and compromise the vulnerable system.

SOLUTION:

These vulnerabilities are fixed in Mozilla Firefox 3.0.12 and Firefox 3.5.1. Firefox 3.0.12 is available for download at Mozilla Firefox 3.0.x Download site (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.12&os=win&lang=en-US) and Firefox 3.5.1 is available for download at Mozilla Firefox 3.5.x Download site (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.1&os=win&lang=en-US).
The vendor has released advisories for each of the vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2009-34 (http://www.mozilla.org/security/announce/2009/mfsa2009-34.html),
MFSA 2009-35 (http://www.mozilla.org/security/announce/2009/mfsa2009-35.html),
MFSA 2009-36 (http://www.mozilla.org/security/announce/2009/mfsa2009-36.html),
MFSA 2009-37 (http://www.mozilla.org/security/announce/2009/mfsa2009-37.html),
MFSA 2009-39 (http://www.mozilla.org/security/announce/2009/mfsa2009-39.html),
MFSA 2009-40 (http://www.mozilla.org/security/announce/2009/mfsa2009-40.html).
Workaround:
CVE-2009-2462, CVE-2009-2463, CVE-2009-2464, CVE-2009-2465, CVE-2009-2466, CVE-2009-2469, CVE-2009-2471, CVE-2009-2472: Disable JavaScript until a version containing these fixes is installed.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.12&os=win&lang=en-US)
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.12&os=linux&lang=en-US)
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.12&os=osx&lang=en-US)
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=win&lang=en-US)
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=linux&lang=en-US)
MFSA 2009-34, MFSA 2009-35, MFSA 2009-36, MFSA 2009-37, MFSA 2009-39, MFSA 2009-40: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2009-2464
Description: Mozilla Firefox 3.0.11 and Thunderbird 2.0.9 - RDF File Handling Remote Memory Corruption - The Exploit-DB Ref : 33101
Link: http://www.exploit-db.com/exploits/33101

exploitdb

Reference: CVE-2009-2464
Description: Mozilla Firefox 3.0.11 and Thunderbird 2.0.9 - RDF File Handling Remote Memory Corruption
Link: https://www.exploit-db.com/exploits/33101

nvd

Reference: CVE-2009-1194
Description: Integer overflow in the pango_glyph_string_set_size function in pango/glyphstring.c in Pango before 1.24 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long glyph string that triggers a heap-based buffer overflow, as demonstrated by a long document.location value in Firefox.
Link: https://bugzilla.redhat.com/show_bug.cgi?id=496887

Reference: CVE-2009-2466
Description: The JavaScript engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsDOMClassInfo.cpp, (2) JS_HashTableRawLookup, and (3) MirrorWrappedNativeParent and js_LockGCThingRT.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=454704

seebug

Reference: CVE-2009-2464
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-86352

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Security Update (MFSA 2009-42,MFSA 2009-43)

| | |
|---|---|
| QID: | 116539 |
| Category: | Local |
| Associated CVEs: | CVE-2009-2408, CVE-2009-2404 |
| Vendor Reference: | MFSA 2009-42, MFSA 2009-43 |
| Bugtraq ID: | 35891 |
| Service Modified: | 08/16/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. The following security vulnerabilities have been reported in Mozilla Firefox:
- Mozilla Firefox before 3.5 and NSS before 3.12.3 do not properly handle a 'DESCRIPTION' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority. (CVE-2009-2408)
- A heap based buffer overflow vulnerability exists in the code that handles regular expressions in certificate names. This vulnerability could be used to compromise the browser and run arbitrary code by presenting a specially crafted certificate to the client. (CVE-2009-2404)
Versions prior to Mozilla Firefox 3.5 are vulnerable.

IMPACT:

If this vulnerability is successfully exploited, it could allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority or compromise the browser and run arbitrary code by presenting a specially crafted certificate to the client.

SOLUTION:

These vulnerabilities are fixed in Mozilla Firefox Version 3.5 or later. Firefox 3.5.1 is available for download at Mozilla Firefox Download site (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.1&os=win&lang=en-US).
The vendor has released advisories for each of the vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2009-42 (http://www.mozilla.org/security/announce/2009/mfsa2009-42.html),
MFSA 2009-43 (http://www.mozilla.org/security/announce/2009/mfsa2009-43.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-42,MFSA 2009-43: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.1&os=win&lang=en-US)
MFSA 2009-42,MFSA 2009-43: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.1&os=osx&lang=en-US)
MFSA 2009-42,MFSA 2009-43: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.1&os=linux&lang=en-US)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Update for 3.5.2 (MFSA 2009-38,MFSA 2009-44,MFSA 2009-45,MFSA 2009-46)

| | |
|---|---|
| QID: | 116542 |
| Category: | Local |
| Associated CVEs: | CVE-2009-2654, CVE-2009-2665, CVE-2009-2470, CVE-2009-2662, CVE-2009-2663, CVE-2009-2664 |
| Vendor Reference: | MFSA 2009-38, MFSA 2009-44, MFSA 2009-45, MFSA 2009-46 |
| Bugtraq ID: | 35928,35925,35803 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. The following security vulnerabilities have been reported in Mozilla Firefox:
- A broken functionality exists on pages that had a Link: HTTP header when an add-on is installed, which implements a Content Policy in JavaScript, such as AdBlock Plus or NoScript. The broken functionality is due to the window's global object receiving an incorrect security wrapper and the issue could be used to execute arbitrary JavaScript with chrome privileges. This issue has been fixed in Firefox 3.5.2 and 3.0.12.
- Several stability bugs were identified in the browser engine used in Firefox and other Mozilla-based products. Some of the crashes can be exploited to cause memory corruption under certain circumstances some could be exploited to run arbitrary code.
- Mozilla Firefox 3.5.1 and earlier allows remote attackers to spoof the address bar, and possibly conduct phishing attacks, via a crafted Web page that calls "window.open" with an invalid character in the URL, makes "document.write" calls to the resulting object, and then calls the stop method during the loading of the error page. (CVE-2009-2654)
- When Firefox receives a reply from a SOCKS5 proxy which contains a DNS name longer than 15 characters, the subsequent data stream in the response can become corrupted. (CVE-2009-2470)
Versions prior to Mozilla Firefox 3.5.2 are vulnerable.

IMPACT:

If this vulnerability is successfully exploited, it could allow attackers to execute arbitrary code.

SOLUTION:

These vulnerabilities are fixed in Mozilla Firefox Version 3.5.2 or later and Version 3.0.13 or later. Firefox 3.5.2 is available for download at Mozilla Firefox 3.5.2 Download site (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=win&lang=en-US).
The vendor has released advisories for each of the vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2009-38 (http://www.mozilla.org/security/announce/2009/mfsa2009-38.html),
MFSA 2009-44 (http://www.mozilla.org/security/announce/2009/mfsa2009-44.html),
MFSA 2009-45 (http://www.mozilla.org/security/announce/2009/mfsa2009-45.html),
MFSA 2009-46 (http://www.mozilla.org/security/announce/2009/mfsa2009-46.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-38,MFSA 2009-44,MFSA 2009-45,MFSA 2009-46: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=win&lang=en-US)
MFSA 2009-38,MFSA 2009-44,MFSA 2009-45,MFSA 2009-46: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=linux&lang=en-US)
MFSA 2009-38,MFSA 2009-44,MFSA 2009-45,MFSA 2009-46: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.2&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2009-2654
- Description: Mozilla Firefox 3.5.1 - Error Page Address Bar URI Spoofing - The Exploit-DB Ref : 33103
- Link: http://www.exploit-db.com/exploits/33103

exploitdb
- Reference: CVE-2009-2654
- Description: Mozilla Firefox 3.5.1 - Error Page Address Bar URI Spoofing
- Link: https://www.exploit-db.com/exploits/33103

nvd
- Reference: CVE-2009-2654
- Description: Mozilla Firefox before 3.0.13, and 3.5.x before 3.5.2, allows remote attackers to spoof the address bar, and possibly conduct phishing attacks, via a crafted web page that calls window.open with an invalid character in the URL, makes document.write calls to the resulting object, and then calls the stop method during the loading of the error page.
- Link: http://www.securityfocus.com/bid/35803

Reference: CVE-2009-2654
Description: Mozilla Firefox before 3.0.13, and 3.5.x before 3.5.2, allows remote attackers to spoof the address bar, and possibly conduct phishing attacks, via a crafted web page that calls window.open with an invalid character in the URL, makes document.write calls to the resulting object, and then calls the stop method during the loading of the error page.
Link: http://www.securityfocus.com/archive/1/505242/30/0/threaded

seebug
Reference: CVE-2009-2654
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-86354

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51)

| | |
|---|---|
| QID: | 116608 |
| Category: | Local |
| Associated CVEs: | CVE-2009-3079, CVE-2009-3078, CVE-2009-3077, CVE-2009-3076, CVE-2009-3069, CVE-2009-3070, CVE-2009-3071, CVE-2009-3072, CVE-2009-3073, CVE-2009-3074, CVE-2009-3075 |
| Vendor Reference: | MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51 |
| Bugtraq ID: | 36343 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. The following security vulnerabilities have been reported in Mozilla Firefox:
- Multiple memory corruption vulnerabilities exist in the browser engine. These issues can be exploited to crash the browser, or possible execute arbitrary code. (CVE-2009-3069, CVE-2009-3070, CVE-2009-3071, CVE-2009-3072, CVE-2009-3073, CVE-2009-3074, CVE-2009-3075)
- A weakness when adding or removing modules with "pkcs11.addmodule" or "pkcs11.deletemodule" results in a dialog not displaying sufficient information. This may aid an attacker in tricking an unsuspecting user into installing a malicious MKCS11 module. (CVE-2009-3076)
- A remote code execution vulnerability exists because the columns of a XUL tree element can be manipulated to point to freed memory. An attacker can exploit this issue to execute arbitrary code; failed exploit attempts will likely result in denial of service conditions. (CVE-2009-3077)
- A vulnerability affects the browser because the default font used to render the location bar, would improperly display certain Unicode characters with a tall line-height. This may aid an attacker obfuscating the URL displayed, and allow other attacks to be conducted. (CVE-2009-3078)
- A privilege-escalation vulnerability affects the "BrowserFeedWriter" because it could be leveraged to run JavaScript code from Web pages with chrome privileges. (CVE-2009-3079)
Versions prior to Mozilla Firefox 3.5.3 and 3.0.14 are vulnerable.

IMPACT:

If these vulnerabilities are successfully exploited, it could allow attackers to obtain potentially sensitive information, execute arbitrary code, gain elevated privileges, and cause denial of service conditions.

SOLUTION:

Workaround:
For CVE-2009-3069, CVE-2009-3070, CVE-2009-3071, CVE-2009-3072, CVE-2009-3073, CVE-2009-3074, CVE-2009-3075, CVE-2009-3079:
- Disable JavaScript until a version containing these fixes can be installed.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.14&os=win&lang=en-US)
MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.14&os=linux&lang=en-US)
MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.14&os=osx&lang=en-US)
MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.3&os=win&lang=en-US)
MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.3&os=linux&lang=en-US)

MFSA 2009-47, MFSA 2009-48, MFSA 2009-49, MFSA 2009-50, MFSA 2009-51: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.3&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2009-3076
Description: Mozilla Firefox < 3.0.14 - Multiplatform Remote Code Execution via pkcs11.addmodule - The Exploit-DB Ref : 9651
Link: http://www.exploit-db.com/exploits/9651

exploitdb
Reference: CVE-2009-3076
Description: Mozilla Firefox < 3.0.14 - Multiplatform Remote Code Execution via pkcs11.addmodule
Link: https://www.exploit-db.com/exploits/9651

seebug
Reference: CVE-2009-3076
Description: Mozilla Firefox < 3.0.14 Multiplatform RCE via pkcs11.addmodule
Link: https://www.seebug.org/vuldb/ssvid-66886

saint
Reference: CVE-2009-3076
Description: Mozilla Firefox PKCS11 Module Installation Code Execution
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_pkcs11

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/SeaMonkey Multiple Vulnerabilities (MFSA 2009-65 through MFSA 2009-71)

| | |
|---|---|
| QID: | 116769 |
| Category: | Local |
| Associated CVEs: | CVE-2009-3987, CVE-2009-3986, CVE-2009-3985, CVE-2009-3984, CVE-2009-3389, CVE-2009-3388, CVE-2009-3979, CVE-2009-3980, CVE-2009-3981, CVE-2009-3982 |
| Vendor Reference: | MFSA 2009-65, MFSA 2009-66, MFSA 2009-67, MFSA 2009-68, MFSA 2009-69, MFSA 2009-70, MFSA 2009-71, RHSA-2009:1674 |
| Bugtraq ID: | 37369,37349,37368,37361,37362,37363,37364,37367,37370,37365,37360 |
| Service Modified: | 08/16/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application. SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The Mozilla Foundation has released multiple advisories regarding security vulnerabilities in Firefox and SeaMonkey. The following issues have been reported:
1) Several flaws were found in the processing of malformed Web content. A Web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. (CVE-2009-3979, CVE-2009-3981, CVE-2009-3986)
2) A flaw was found in the Firefox NT Lan Manager (NTLM) authentication protocol implementation. If an attacker could trick a local user that has NTLM credentials into visiting a specially-crafted Web page, they could send arbitrary requests, authenticated with the user's NTLM credentials, to other applications on the user's system. (CVE-2009-3983)
3) A flaw was found in the way Firefox displayed the SSL location bar indicator. An attacker could create an unencrypted Web page that appears to be encrypted, possibly tricking the user into believing they are visiting a secure page. (CVE-2009-3984)
4) A flaw was found in the way Firefox displayed blank pages after a user navigates to an invalid address. If a user visits an attacker-controlled Web page that results in a blank page, the attacker could inject content into that blank page, possibly tricking the user into believing they are viewing a legitimate page. (CVE-2009-3985)
Versions prior to Mozilla Firefox 3.5.6 / 3.0.16 and SeaMonkey 2.0.1 are vulnerable.

IMPACT:

Successful exploitation allows attackers to crash the application or execute arbitrary code.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2009-65 (http://www.mozilla.org/security/announce/2009/mfsa2009-65.html),
MFSA 2009-66 (http://www.mozilla.org/security/announce/2009/mfsa2009-66.html),
MFSA 2009-67 (http://www.mozilla.org/security/announce/2009/mfsa2009-67.html),
MFSA 2009-68 (http://www.mozilla.org/security/announce/2009/mfsa2009-68.html),
MFSA 2009-69 (http://www.mozilla.org/security/announce/2009/mfsa2009-69.html),
MFSA 2009-70 (http://www.mozilla.org/security/announce/2009/mfsa2009-70.html),
MFSA 2009-71 (http://www.mozilla.org/security/announce/2009/mfsa2009-71.html).
For Red Hat:
Refer to Red Hat security advisory RHSA-2009-1674 (https://rhn.redhat.com/errata/RHSA-2009-1674.html) to address this issue and obtain further details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Windows (Firefox)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=win&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Linux (Firefox)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=linux&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Mac OS (Firefox)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=osx&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.6&os=win&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.6&os=linux&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.6&os=osx&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Windows (SeaMonkey)
(http://download.mozilla.org/?product=seamonkey-2.0.1&os=win&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Linux (SeaMonkey)
(http://download.mozilla.org/?product=seamonkey-2.0.1&os=linux&lang=en-US)
MFSA 2009-65,MFSA 2009-66,MFSA 2009-67,MFSA 2009-68,MFSA 2009-69,MFSA 2009-70,MFSA 2009-71: Mac OS (SeaMonkey)
(http://download.mozilla.org/?product=seamonkey-2.0.1&os=osx&lang=en-US)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 4 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities (MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05)

| | |
|---|---|
| QID: | 116903 |
| Category: | Local |
| Associated CVEs: | CVE-2009-1571, CVE-2009-3988, CVE-2010-0159, CVE-2010-0160, CVE-2010-0162 |
| Vendor Reference: | MFSA 2010-01, MFSA 2010-02, MFSA 2010-03, MFSA 2010-04, MFSA 2010-05 |
| Bugtraq ID: | - |
| Service Modified: | 08/05/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozillla applications are prone to the following vulnerabilities:
- An error exists when handling out of memory conditions. This can be exploited to trigger a memory corruption and execute arbitrary code via a specially crafted Web

page.
- Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
- An error exists in the implementation of Web Worker array data types when processing posted messages. This can be exploited to corrupt memory and potentially execute arbitrary code.
- An error exists in the implementation of the "showModalDialog()" function. This can be exploited to potentially execute arbitrary JavaScript code in the context of a domain calling the affected function with external parameters.
- An error exists when processing SVG documents served with a Content Type of "application/octet-stream". This can be exploited to execute arbitrary JavaScript code in the context of a domain hosting the SVG document.
Affected Software:
Firefox 3.5.x versions prior to 3.5.8
Firefox versions prior to 3.0.18
Thunderbird versions prior to 3.0.2
SeaMonkey versions prior to 2.0.3

IMPACT:

Successful exploitation allows malicious people to conduct cross-site scripting attacks, execute arbitrary code and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-01 (http://www.mozilla.org/security/announce/2010/mfsa2010-01.html), MFSA 2010-02 (http://www.mozilla.org/security/announce/2010/mfsa2010-02.html), MFSA 2010-03 (http://www.mozilla.org/security/announce/2010/mfsa2010-03.html), MFSA 2010-04 (http://www.mozilla.org/security/announce/2010/mfsa2010-04.html), MFSA 2010-05 (http://www.mozilla.org/security/announce/2010/mfsa2010-05.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.18&os=win&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.18&os=osx&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.18&os=linux&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.8&os=linux&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.8&os=win&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.8&os=osx&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6&os=linux&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6&os=win&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Mac OS X (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6&os=osx&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Windows (SeaMoneky)
(http://download.mozilla.org/?product=seamonkey-2.0.3&os=win&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Linux (SeaMoneky)
(http://download.mozilla.org/?product=seamonkey-2.0.3&os=linux&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Mac OS (SeaMoneky)
(http://download.mozilla.org/?product=seamonkey-2.0.3&os=osx&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Windows (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=win&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Linux (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=linux&lang=en-US)
MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05: Mac OS X (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.2&os=osx&lang=en-US)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Plugin Parameter Array Dangling Pointer Vulnerability (MFSA 2010-48)

QID: 118305

| | |
|---|---|
| Category: | Local |
| Associated CVEs: | CVE-2010-2755 |
| Vendor Reference: | MFSA 2010-48 |
| Bugtraq ID: | - |
| Service Modified: | 07/28/2010 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application.
The fix to the plugin parameter array crash that was fixed in Firefox 3.6.7 caused a crash showing signs of memory corruption. In certain circumstances, properties in the plugin instance's parameter array could be freed prematurely leaving a dangling pointer that the plugin could execute, potentially calling into attacker-controlled memory. (CVE-2010-2755)
Mozilla Firefox Versions prior to 3.6.8 are vulnerable.

IMPACT:

Successful exploitation allows attackers to cause a crash showing signs of memory corruption.

SOLUTION:

This issue have been fixed in Firefox 3.6.8 and later. The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-48 (http://www.mozilla.org/security/announce/2010/mfsa2010-48.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-48: Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.7&os=win&lang=en-US)
MFSA 2010-48: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.7&os=osx&lang=en-US)
MFSA 2010-48: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.7&os=linux&lang=en-US)

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  1.7.0.0

### 4 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities (MFSA 2010-49 through MFSA 2010-63)

| | |
|---|---|
| QID: | 118485 |
| Category: | Local |
| Associated CVEs: | CVE-2010-2760, CVE-2010-2762, CVE-2010-2763, CVE-2010-2764, CVE-2010-2765, CVE-2010-2766, CVE-2010-2767, CVE-2010-2768, CVE-2010-2769, CVE-2010-2770, CVE-2010-3166, CVE-2010-3167, CVE-2010-3168, CVE-2010-3169, CVE-2010-3131 |
| Vendor Reference: | MSFA2010-49, MSFA2010-50, MSFA2010-51, MSFA2010-52, MSFA2010-53, MSFA2010-54, MSFA2010-55, MSFA2010-56, MSFA2010-57, MSFA2010-58, MSFA2010-59, MSFA2010-60, MSFA2010-61, MSFA2010-62, MSFA2010-63 |
| Bugtraq ID: | 43092,43104,43095,43100,43101,43106,43102,43097,43108,43118 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to the following vulnerabilities:

1) Some unspecified errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
2) An integer overflow error within the implementation of the HTML frameset element can be exploited to cause a heap-based buffer overflow by passing a very large number of columns in the counter for the column numbers.
3) An error in the implementation of "navigator.plugins" can be exploited to trigger the use of an invalid pointer and execute arbitrary code.
4) An error when transforming text runs can be exploited to cause a heap-based buffer overflow via a specially crafted page containing bidirectional text run.
5) A use after free error in the handling of XUL tree selections can be exploited to corrupt memory and execute arbitrary code.
6) An error in the handling of XUL tree objects can be exploited to trigger the removal of the tree from the DOM and cause certain sections of deleted memory to be accessed.
7) An error in the handling of "nsTreeContentView" can be exploited to remove a node before accessing it.
Affected Software:
Firefox 3.6.x Versions prior to 3.6.9
Firefox Versions prior to 3.5.12
Thunderbird 3.1.x Versions prior to 3.1.3
Thunderbird Versions prior to 3.0.7
SeaMonkey Versions prior to 2.0.7

IMPACT:

Successful exploitation allows malicious people to to disclose potentially sensitive information, conduct cross-site scripting attacks, or compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-49 (http://www.mozilla.org/security/announce/2010/mfsa2010-49.html), MFSA 2010-50 (http://www.mozilla.org/security/announce/2010/mfsa2010-50.html), MFSA 2010-51 (http://www.mozilla.org/security/announce/2010/mfsa2010-51.html), MFSA 2010-52 (http://www.mozilla.org/security/announce/2010/mfsa2010-52.html), MFSA 2010-53 (http://www.mozilla.org/security/announce/2010/mfsa2010-53.html), MFSA 2010-54 (http://www.mozilla.org/security/announce/2010/mfsa2010-54.html), MFSA 2010-55 (http://www.mozilla.org/security/announce/2010/mfsa2010-55.html), MFSA 2010-56 (http://www.mozilla.org/security/announce/2010/mfsa2010-56.html), MFSA 2010-57 (http://www.mozilla.org/security/announce/2010/mfsa2010-57.html), MFSA 2010-58 (http://www.mozilla.org/security/announce/2010/mfsa2010-58.html), MFSA 2010-59 (http://www.mozilla.org/security/announce/2010/mfsa2010-59.html), MFSA 2010-60 (http://www.mozilla.org/security/announce/2010/mfsa2010-60.html), MFSA 2010-61 (http://www.mozilla.org/security/announce/2010/mfsa2010-61.html), MFSA 2010-62 (http://www.mozilla.org/security/announce/2010/mfsa2010-62.html), MFSA 2010-63 (http://www.mozilla.org/security/announce/2010/mfsa2010-63.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.9&os=linux&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Linux (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.3&os=linux&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Linux (Sea Monkey)
(http://download.mozilla.org/?product=seamonkey-2.0.7&os=linux&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.9&os=osx&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Mac OS  (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.3&os=osx&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Mac OS (Sea Monkey)
(http://download.mozilla.org/?product=seamonkey-2.0.7&os=osx&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.9&os=win&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Windows (Thunderbird)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.3&os=win&lang=en-US)
MFSA 2010-49,MFSA 2010-50,MFSA 2010-51,MFSA 2010-52,MFSA 2010-53,MFSA 2010-54,MFSA 2010-55,MFSA 2010-56,MFSA 2010-57,MFSA 2010-58,MFSA 2010-59,MFSA 2010-60,MFSA 2010-61,MFSA 2010-62,MFSA 2010-63: Windows (Sea Monkey)
(http://download.mozilla.org/?product=seamonkey-2.0.7&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security
Reference: CVE-2010-3131
Description: Mozilla Thunderbird dwmapi DLL Hijacking Exploit - Core Security Category : Exploits/Client Side

The Exploit-DB
Reference: CVE-2010-3131
Description: Mozilla Firefox 3.6.8 - 'dwmapi.dll' DLL Hijacking - The Exploit-DB Ref : 14730
Link: http://www.exploit-db.com/exploits/14730

Reference: CVE-2010-3131
Description: Mozilla Thunderbird - 'dwmapi.dll' DLL Hijacking - The Exploit-DB Ref : 14783
Link: http://www.exploit-db.com/exploits/14783

exploitdb
Reference: CVE-2010-3131
Description: Mozilla Firefox 3.6.8 - 'dwmapi.dll' DLL Hijacking
Link: https://www.exploit-db.com/exploits/14730

Reference: CVE-2010-3131
Description: Mozilla Thunderbird - 'dwmapi.dll' DLL Hijacking
Link: https://www.exploit-db.com/exploits/14783

nvd
Reference: CVE-2010-3131
Description: Untrusted search path vulnerability in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 on Windows XP allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a .htm, .html, .jtx, .mfp, or .eml file.
Link: http://www.exploit-db.com/exploits/14730

Reference: CVE-2010-3131
Description: Untrusted search path vulnerability in Mozilla Firefox before 3.5.12 and 3.6.x before 3.6.9, Thunderbird before 3.0.7 and 3.1.x before 3.1.3, and SeaMonkey before 2.0.7 on Windows XP allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a .htm, .html, .jtx, .mfp, or .eml file.
Link: http://www.exploit-db.com/exploits/14783

seebug
Reference: CVE-2010-3131
Description: Mozilla Thunderbird DLL Hijacking Exploit (dwmapi.dll)
Link: https://www.seebug.org/vuldb/ssvid-69700

Reference: CVE-2010-3131
Description: Firefox
Link: https://www.seebug.org/vuldb/ssvid-69657

coreimpact
Reference: CVE-2010-3131
Description: Mozilla Thunderbird dwmapi DLL Hijacking Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox 3.5/3.6 Unspecified Remote Code Execution Vulnerability (MFSA 2010-73)

| | |
|---|---|
| QID: | 118660 |
| Category: | Local |
| Associated CVEs: | CVE-2010-3765 |
| Vendor Reference: | MSFA 2010-73 |
| Bugtraq ID: | 44425 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application for multiple operating systems.
Mozilla Firefox is prone to a unspecified remote code-execution vulnerability.
Firefox 3.5.x and 3.6.x are vulnerable.

IMPACT:

Successful exploits will allow an attacker to run arbitrary code in the context of the user running the application. Failed attacks may cause denial of service.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-73 (http://www.mozilla.org/security/announce/2010/mfsa2010-73.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-73: Linux (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.10&os=linux&lang=en-US)
MFSA 2010-73: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.6&os=linux&lang=en-US)
MFSA 2010-73: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.12&os=linux&lang=en-US)
MFSA 2010-73: MacOs (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.10&os=osx&lang=en-US)
MFSA 2010-73: MacOs (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.12&os=osx&lang=en-US)
MFSA 2010-73: MacOs (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.6&os=osx&lang=en-US)
MFSA 2010-73: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.12&os=win&lang=en-US)
MFSA 2010-73: Windows (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.10&os=win&lang=en-US)
MFSA 2010-73: Windows (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.6&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Immunity

Reference: CVE-2010-3765
Description: firefox_appendchild - Immunity Ref : firefox_appendchild
Link: http://immunityinc.com

Metasploit

Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaved document.write/appendChild Memory Corruption - Metasploit Ref : /modules/exploit/windows/browser/mozilla_interleaved_write
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_interleaved_write.rb

Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaved document.write/appendChild Memory Corruption - Metasploit Ref : /modules/exploit/linux/local/rds_rds_page_copy_user_priv_esc
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_interleaved_write.rb

The Exploit-DB

Reference: CVE-2010-3765
Description: Mozilla Firefox - Interleaving 'document.write' / 'appendChild' (Metasploit) - The Exploit-DB Ref : 16509
Link: http://www.exploit-db.com/exploits/16509

Reference: CVE-2010-3765
Description: Mozilla Firefox - Interleaving 'document.write' / 'appendChild' Denial of Service - The Exploit-DB Ref : 15341
Link: http://www.exploit-db.com/exploits/15341

Reference: CVE-2010-3765
Description: Mozilla Firefox - Simplified Memory Corruption (PoC) - The Exploit-DB Ref : 15342
Link: http://www.exploit-db.com/exploits/15342

Reference: CVE-2010-3765
Description: Mozilla Firefox 3.6.8 < 3.6.11 - Interleaving 'document.write' / 'appendChild' Remote Overflow - The Exploit-DB Ref : 15352
Link: http://www.exploit-db.com/exploits/15352

exploitdb

Reference: CVE-2010-3765
Description: Mozilla Firefox - Simplified Memory Corruption (PoC)
Link: https://www.exploit-db.com/exploits/15342

Reference: CVE-2010-3765
Description: Mozilla Firefox - Interleaving 'document.write' / 'appendChild' (Metasploit)
Link: https://www.exploit-db.com/exploits/16509

Reference: CVE-2010-3765
Description: Mozilla Firefox - Interleaving 'document.write' / 'appendChild' Denial of Service
Link: https://www.exploit-db.com/exploits/15341

Reference: CVE-2010-3765
Description: Mozilla Firefox 3.6.8 < 3.6.11 - Interleaving 'document.write' / 'appendChild' Remote Overflow
Link: https://www.exploit-db.com/exploits/15352

nvd

Reference: CVE-2010-3765
Description: Mozilla Firefox 3.5.x through 3.5.14 and 3.6.x through 3.6.11, Thunderbird 3.1.6 before 3.1.6 and 3.0.x before 3.0.10, and SeaMonkey 2.x before 2.0.10, when JavaScript is enabled, allows remote attackers to execute arbitrary code via vectors related to nsCSSFrameConstructor::ContentAppended, the appendChild method, incorrect index tracking, and the creation of multiple frames, which triggers memory corruption, as exploited in the wild in October 2010 by the Belmoo malware.
Link: http://www.exploit-db.com/exploits/15352

Reference: CVE-2010-3765
Description: Mozilla Firefox 3.5.x through 3.5.14 and 3.6.x through 3.6.11, Thunderbird 3.1.6 before 3.1.6 and 3.0.x before 3.0.10, and SeaMonkey 2.x before 2.0.10, when JavaScript is enabled, allows remote attackers to execute arbitrary code via vectors related to nsCSSFrameConstructor::ContentAppended, the appendChild method, incorrect index tracking, and the creation of multiple frames, which triggers memory corruption, as exploited in the wild in October 2010 by the Belmoo malware.
Link: http://www.exploit-db.com/exploits/15341

Reference: CVE-2010-3765
Description: Mozilla Firefox 3.5.x through 3.5.14 and 3.6.x through 3.6.11, Thunderbird 3.1.6 before 3.1.6 and 3.0.x before 3.0.10, and SeaMonkey 2.x before 2.0.10, when JavaScript is enabled, allows remote attackers to execute arbitrary code via vectors related to nsCSSFrameConstructor::ContentAppended, the appendChild method, incorrect index tracking, and the creation of multiple frames, which triggers memory corruption, as exploited in the wild in October 2010 by the Belmoo malware.
Link: http://www.exploit-db.com/exploits/15342

seebug

Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaving document.write and appendChild Exploit
Link: https://www.seebug.org/vuldb/ssvid-71023

Reference: CVE-2010-3765
Description: Firefox 3.6.8 - 3.6.11 Interleaving document.write and appendChild Exploit (From the Wild)
Link: https://www.seebug.org/vuldb/ssvid-70088

saint

Reference: CVE-2010-3765
Description: Mozilla Firefox document.write and DOM insertion memory corruption
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_document_write_dom

packetstorm

Reference: CVE-2010-3765
Description: Firefox Memory Corruption
Link: https://packetstormsecurity.com/files/95278/Firefox-Memory-Corruption.html

Reference: CVE-2010-3765
Description: Firefox Interleaving Denial Of Service
Link: https://packetstormsecurity.com/files/95201/Firefox-Interleaving-Denial-Of-Service.html

Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaving document.write / appendChild Code Execution
Link: https://packetstormsecurity.com/files/98589/Mozilla-Firefox-Interleaving-document.write-appendChild-Code-Execution.html

canvas

Reference: CVE-2010-3765

Description: firefox_appendchild
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/firefox_appendchild

metasploit
Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaved document.write/appendChild Memory Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2010-3765
Description: Mozilla Firefox Interleaved document.write/appendChild Memory Corruption
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/mozilla_interleaved_write.rb

ASSOCIATED MALWARE:

Trend Micro
Malware ID: HTML_SHELLCOD.SM
Risk: Low
Type: Trojan
Platform: Windows 2000; Windows XP; Windows Server 2003
Link: http://about-threats.trendmicro.com/Malware.aspx?name=HTML_SHELLCOD.SM&language=us

ReversingLabs
Malware ID: MetaSploit
Type: Hacktool
Platform: Script

Malware ID: Pdfjsc
Type: Exploit
Platform: Document

Malware ID: BlackHole
Type: Exploit
Platform: Script

Malware ID: CVE-2010-3765
Type: Exploit
Platform: DOS,MacOS,Binary,Document,Script

Malware ID: Evisnefo
Type: Exploit
Platform: Win32

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox SeaMonkey Thunderbird Multiple Vulnerabilities (MFSA2010-74 through MFSA2010-84)

| | |
|---|---|
| QID: | 118823 |
| Category: | Local |
| Associated CVEs: | CVE-2010-3766, CVE-2010-3767, CVE-2010-3768, CVE-2010-3769, CVE-2010-3770, CVE-2010-3771, CVE-2010-3772, CVE-2010-3773, CVE-2010-3774, CVE-2010-3775, CVE-2010-3776, CVE-2010-3777, CVE-2010-3778 |
| Vendor Reference: | mfsa2010-74, mfsa2010-75, mfsa2010-76, mfsa2010-77, mfsa2010-78, mfsa2010-79, mfsa2010-80, mfsa2010-81, mfsa2010-82, mfsa2010-83, mfsa2010-84 |
| Bugtraq ID: | 45353,45346,45351,45355,45347,45348,45344,45326,45345,45352,45354 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |

Edited: No
PCI Vuln: Yes

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to the following vulnerabilities:
- Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
- An error when handling line breaks in overly long strings passed to "document.write()" can be exploited to read data from out-of-bounds memory location and potentially execute arbitrary code.
- An error when opening a new window using "window.open()" can be exploited to execute arbitrary JavaScript code with chrome privileges via the "isindex" element.
- An error in the handling of "div" elements nested within "treechildren" elements in a XUL tree element can be exploited to corrupt memory and potentially execute arbitrary code.
- An error in the Java LiveConnect script when loaded via a "data:" URL can be exploited to e.g. read arbitrary files, launch arbitrary processes, and establish arbitrary network connections.
- A use-after-free error in the "NodeIterator API" when handling a "nsDOMAttribute" node can be exploited to corrupt memory and execute arbitrary code.
- An integer overflow when creating arrays can be exploited to corrupt memory and potentially execute arbitrary code.
- An error related to the XMLHttpRequestSpy object can be exploited to execute arbitrary JavaScript code.
- An error exists in the handling of documents with no inherent origin associated. This can be exploited to bypass the same-origin policy and spoof the URL of a trusted site by tricking users into opening site which result in e.g. about:config or about:neterror pages.
- An error exists in the rendering engine when handling certain Mac charset encodings. This can be exploited to potentially execute arbitrary JavaScript code in the context of the destination Web site.
Affected Software:
Firefox prior to 3.5.16
Firefox 3.6.x versions prior to 3.6.13
Thunderbird prior to 3.0.11
Thunderbird 3.1.x versions prior to 3.1.7
SeaMonkey prior to 2.0.11

IMPACT:

Successful exploitation allows malicious people to conduct cross-site scripting and spoofing attacks, bypass certain security restrictions, and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA2010-74 (http://www.mozilla.org/security/announce/2010/mfsa2010-74.html),MFSA2010-75 (http://www.mozilla.org/security/announce/2010/mfsa2010-75.html),MFSA2010-76 (http://www.mozilla.org/security/announce/2010/mfsa2010-76.html),MFSA2010-77 (http://www.mozilla.org/security/announce/2010/mfsa2010-77.html),MFSA2010-78 (http://www.mozilla.org/security/announce/2010/mfsa2010-78.html),MFSA2010-79 (http://www.mozilla.org/security/announce/2010/mfsa2010-79.html),MFSA2010-80 (http://www.mozilla.org/security/announce/2010/mfsa2010-80.html),MFSA2010-81 (http://www.mozilla.org/security/announce/2010/mfsa2010-81.html),MFSA2010-82 (http://www.mozilla.org/security/announce/2010/mfsa2010-82.html),MFSA2010-83 (http://www.mozilla.org/security/announce/2010/mfsa2010-83.html),MFSA2010-84 (http://www.mozilla.org/security/announce/2010/mfsa2010-84.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2010-74 through MFSA2010-84: Windows (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.13&os=win&lang=en-US)
MFSA2010-74 through MFSA2010-84: Windows (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.16&os=win&lang=en-US)
MFSA2010-74 through MFSA2010-84: Linux (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.13&os=linux&lang=en-US)
MFSA2010-74 through MFSA2010-84: Linux (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.16&os=linux&lang=en-US)
MFSA2010-74 through MFSA2010-84: Mac OS (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.13&os=osx&lang=en-US)
MFSA2010-74 through MFSA2010-84: Mac OS (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.16&os=osx&lang=en-US)
MFSA2010-74 through MFSA2010-84: Windows (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.7&os=win&lang=en-US)
MFSA2010-74 through MFSA2010-84: Windows (Thunderbird 3.0) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.11&os=win&lang=en-US)
MFSA2010-74 through MFSA2010-84: Linux (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.7&os=linux&lang=en-US)
MFSA2010-74 through MFSA2010-84: Linux (Thunderbird 3.0) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.11&os=linux&lang=en-US)
MFSA2010-74 through MFSA2010-84: Mac OS (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.7&os=osx&lang=en-US)
MFSA2010-74 through MFSA2010-84: Mac OS (Thunderbird 3.0) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.11&os=osx&lang=en-US)
MFSA2010-74 through MFSA2010-84: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.11&os=win&lang=en-US)
MFSA2010-74 through MFSA2010-84: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.11&os=linux&lang=en-US)
MFSA2010-74 through MFSA2010-84: Mac OS (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.11&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2010-3770

Description: Mozilla Firefox/Thunderbird/SeaMonkey - Multiple HTML Injection Vulnerabilities - The Exploit-DB Ref : 35095

Link: http://www.exploit-db.com/exploits/35095

exploitdb

Reference: CVE-2010-3770

Description: Mozilla Firefox/Thunderbird/SeaMonkey - Multiple HTML Injection Vulnerabilities

Link: https://www.exploit-db.com/exploits/35095

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA 2011-12 through MFSA 2011-18)

| | |
|---|---|
| QID: | 119217 |
| Category: | Local |
| Associated CVEs: | CVE-2011-0066, CVE-2011-0067, CVE-2011-0069, CVE-2011-0070, CVE-2011-0071, CVE-2011-0072, CVE-2011-0073, CVE-2011-0074, CVE-2011-0075, CVE-2011-0076, CVE-2011-0077, CVE-2011-0078, CVE-2011-0080, CVE-2011-0081, CVE-2011-1202, CVE-2011-0068, CVE-2011-0079 |
| Vendor Reference: | mfsa2011-12, mfsa2011-13, mfsa2011-14, mfsa2011-15, mfsa2011-16, mfsa2011-17, mfsa2011-18 |
| Bugtraq ID: | 46785,47655,47646,47647,47648,47651,47641,47653,47656,47654 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client. SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to the following vulnerabilities:
- Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
- Multiple use-after-free errors within the handling of the "mChannel", "mObserverList", and "nsTreeRange" object attributes can be exploited to execute arbitrary code.
- An error when handling Java applets can be exploited to steal entries from the form history via the autocomplete controls.
- An error within the Java Embedding Plugin (JEP) can be exploited to gain escalated privileges.
- An error in the implementation of the "resource:" protocol can be exploited to perform directory traversal attacks and disclose sensitive information.
- An error in the WebGLES library when loading a shader can be exploited to cause a buffer overflow and execute arbitrary code.
- An off-by-three error in libGLESv2 can be exploited to corrupt memory and execute arbitrary code.
Affected Versions:
Firefox 4.0, Firefox 3.0.x, Firefox 3.6.x prior to 3.6.17, Firefox 3.5.x prior to 3.5.19; Thunderbird prior to 3.1.10; SeaMonkey prior to 2.0.14

IMPACT:

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

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2011-02 (http://www.mozilla.org/security/announce/2011/mfsa2011-12.html), MFSA 2011-13 (http://www.mozilla.org/security/announce/2011/mfsa2011-13.html), MFSA2011-14 (http://www.mozilla.org/security/announce/2011/mfsa2011-14.html), MFSA2011-15 (http://www.mozilla.org/security/announce/2011/mfsa2011-15.html), MFSA2011-16 (http://www.mozilla.org/security/announce/2011/mfsa2011-16.html), MFSA2011-17 (http://www.mozilla.org/security/announce/2011/mfsa2011-17.html), MFSA2011-18 (http://www.mozilla.org/security/announce/2011/mfsa2011-18.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2011-12 through MFSA 2011-13: Linux (Firefox 3.6) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.17&os=linux&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.14&os=linux&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Linux (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.10&os=linux&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Linux (Firefox 3.5) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.19&os=linux&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Mac OS (Thunderbird 3.1) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.10&os=osx&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Windows (Thunderbird 3.1)

(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.17&os=osx&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Mac OS (Firefox 3.5)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.19&os=win&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Mac OS (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.14&os=osx&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Windows (Firefox 3.6)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.17&os=win&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.14&os=win&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Windows (Firefox 3.5)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.19&os=win&lang=en-US)
MFSA 2011-12 through MFSA 2011-13: Mac OS (Firefox 3.6)
(http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.10&os=win&lang=en-US)
MFSA 2011-12, MFSA 2011-17, MSA 2011-18: Windows (Firefox 4.1) (http://www.mozilla.com/en-US/firefox/fx/)
MFSA 2011-12, MFSA 2011-17, MSA 2011-18: Mac OS (Firefox 4.1) (http://www.mozilla.com/en-US/firefox/fx/)
MFSA 2011-12, MFSA 2011-17, MSA 2011-18: Linux (Firefox 4.1) (http://www.mozilla.com/en-US/firefox/fx/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability - Metasploit Ref : /modules/exploit/windows/browser/mozilla_nstreerange
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_nstreerange.rb

The Exploit-DB

Reference: CVE-2011-0073
Description: Mozilla Firefox - 'nsTreeRange' Dangling Pointer (2) - The Exploit-DB Ref : 17419
Link: http://www.exploit-db.com/exploits/17419

Reference: CVE-2011-0073
Description: Mozilla Firefox - 'nsTreeRange' Dangling Pointer (Metasploit) (1) - The Exploit-DB Ref : 17520
Link: http://www.exploit-db.com/exploits/17520

exploitdb

Reference: CVE-2011-0073
Description: Mozilla Firefox - 'nsTreeRange' Dangling Pointer (2)
Link: https://www.exploit-db.com/exploits/17419

Reference: CVE-2011-0073
Description: Mozilla Firefox - 'nsTreeRange' Dangling Pointer (Metasploit) (1)
Link: https://www.exploit-db.com/exploits/17520

nvd

Reference: CVE-2011-0067
Description: Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, and SeaMonkey before 2.0.14, does not properly implement autocompletion for forms, which allows remote attackers to read form history entries via a Java applet that spoofs interaction with the autocomplete controls.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=527935

Reference: CVE-2011-0069
Description: Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1; Thunderbird before 3.1.10; and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0070.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=644069

Reference: CVE-2011-0070
Description: Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.19, 3.6.x before 3.6.17, and 4.x before 4.0.1; Thunderbird before 3.1.10; and SeaMonkey before 2.0.14 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0069.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=645565

Reference: CVE-2011-0071
Description: Directory traversal vulnerability in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17, Thunderbird before 3.1.10, and SeaMonkey before 2.0.14 on Windows allows remote attackers to determine the existence of arbitrary files, and possibly load resources, via vectors involving a resource: URL.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=624764

Reference: CVE-2011-1202
Description: The xsltGenerateIdFunction function in functions.c in libxslt 1.1.26 and earlier, as used in Google Chrome before 10.0.648.127 and other products, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function.
Link: http://code.google.com/p/chromium/issues/detail?id=73716

Reference: CVE-2011-0079
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 4.x before 4.0.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to gfx/layers/d3d10/ReadbackManagerD3D10.cpp and unknown other vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=639885

seebug
Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability
Link: https://www.seebug.org/vuldb/ssvid-71871

Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Exploit
Link: https://www.seebug.org/vuldb/ssvid-71794

saint
Reference: CVE-2011-0073
Description: Mozilla Firefox nsTreeRange Use After Free
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_nstreerange_uaf

packetstorm
Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability
Link: https://packetstormsecurity.com/files/102948/Mozilla-Firefox-nsTreeRange-Dangling-Pointer-Vulnerability.html

metasploit
Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2011-0073
Description: Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/mozilla_nstreerange.rb

white-phosphorus
Reference: CVE-2011-0073
Description: wp_mozilla_firefox_nstreerange
Link: http://exploitlist.immunityinc.com/home/exploitpack/White_Phosphorus/wp_mozilla_firefox_nstreerange

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: Meterpreter
Type: Backdoor
Platform: Script

Malware ID: Leivion
Type: Trojan
Platform: Script,Win32

Malware ID: CVE-2015-2419
Type: Exploit
Platform: Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA 2011-29 through MFSA 2011-33)

| | |
|---|---|
| QID: | 119516 |
| Category: | Local |
| Associated CVEs: | CVE-2011-2993, CVE-2011-2992, CVE-2011-2991, CVE-2011-2990, CVE-2011-2989, CVE-2011-2988, CVE-2011-2987, CVE-2011-2986, CVE-2011-2985, CVE-2011-2984, CVE-2011-2983, CVE-2011-2982, CVE-2011-2981, CVE-2011-2980, CVE-2011-2978, CVE-2011-0084 |
| Vendor Reference: | MFSA2011-29, MFSA2011-30, MFSA2011-31, MFSA2011-32, MFSA2011-33 |
| Bugtraq ID: | 49166,49226,49242,49042 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
The Mozilla Foundation has released multiple security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird and SeaMonkey. Mozilla Firefox, Thunderbird and SeaMonkey are exposed to the multiple remote vulnerabilities. See reference for further details.
Affected Versions:
Firefox prior to 3.6.20
Firefox prior to 6
Thunderbird prior to 3.1.12
Thunderbird prior to 6
SeaMonkey prior to 2.3

IMPACT:

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

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2011-29 (http://www.mozilla.org/security/announce/2011/mfsa2011-29.html), MFSA 2011-30 (http://www.mozilla.org/security/announce/2011/mfsa2011-30.html), MFSA2011-31 (http://www.mozilla.org/security/announce/2011/mfsa2011-31.html), MFSA2011-32 (http://www.mozilla.org/security/announce/2011/mfsa2011-32.html), MFSA2011-33 (http://www.mozilla.org/security/announce/2011/mfsa2011-33.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2011-19 through MFSA2011-29: Linux (Firefox 3.6.20) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.20&os=linux&lang=en-US)
MFSA2011-19 through MFSA2011-29: Linux (Firefox 6.0) (http://download.mozilla.org/?product=firefox-6.0&os=linux&lang=en-US)
MFSA2011-19 through MFSA2011-29: Linux (Thunderbird 3.1.12) (http://download.mozilla.org/?product=thunderbird-3.1.12&os=linux&lang=en-US)
MFSA2011-19 through MFSA2011-29: Mac OS X (Firefox 3.6.20) (http://download.mozilla.org/?product=firefox-3.6.20&os=osx&lang=en-US)
MFSA2011-19 through MFSA2011-29: Mac OS X (Firefox 6.0) (http://download.mozilla.org/?product=firefox-6.0&os=osx&lang=en-US)
MFSA2011-19 through MFSA2011-29: Mac OS X (Thunderbird 3.1.12) (http://download.mozilla.org/?product=thunderbird-3.1.12&os=osx&lang=en-US)
MFSA2011-19 through MFSA2011-29: Windows (Firefox 3.6.20) (http://download.mozilla.org/?product=firefox-3.6.20&os=win&lang=en-US)
MFSA2011-19 through MFSA2011-29: Windows (Firefox 6.0) (http://download.mozilla.org/?product=firefox-6.0&os=win&lang=en-US)
MFSA2011-19 through MFSA2011-29: Windows 2000 (can be applied to Gold, Service Pack 1, and Service Pack 2) (Thunderbird 3.1.12) (http://download.mozilla.org/?product=thunderbird-3.1.12&os=win&lang=en-US)
MFSA2011-19 through MFSA2011-29: Linux (Seamonkey 2.3) (http://download.mozilla.org/?product=seamonkey-2.3&os=linux&lang=en-US)
MFSA2011-19 through MFSA2011-29: Mac OS X (Seamonkey 2.3) (http://download.mozilla.org/?product=seamonkey-2.3&os=osx&lang=en-US)
MFSA2011-19 through MFSA2011-29: Windows (Seamonkey 2.3) (http://download.mozilla.org/?product=seamonkey-2.3&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

saint
Reference: CVE-2011-2980
Description: Firefox sensor.dll Insecure Library Loading
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_insecure_library_load_sensor

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA-2011-36 through MFSA-2011-45)

| | |
|---|---|
| QID: | 119622 |
| Category: | Local |
| Associated CVEs: | CVE-2011-2372, CVE-2011-2995, CVE-2011-2996, CVE-2011-2997, CVE-2011-2999, CVE-2011-3000, CVE-2011-3001, CVE-2011-3002, CVE-2011-3003, CVE-2011-3005, CVE-2011-3232 |
| Vendor Reference: | MFSA2011-36, MFSA2011-37, MFSA2011-38, MFSA2011-39, MFSA2011-40, MFSA2011-41, MFSA2011-42, MFSA2011-43, MFSA2011-44, MFSA2011-45 |
| Bugtraq ID: | - |
| Service Modified: | 12/09/2014 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
The Mozilla Foundation has released multiple security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird and SeaMonkey. Mozilla Firefox, Thunderbird and SeaMonkey are exposed to the multiple remote vulnerabilities. See reference for further details.
Affected Versions:
Firefox prior to 3.6.23
Firefox prior to 7.0
Thunderbird prior to 7.0
SeaMonkey prior to 2.4

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to execute arbitrary code.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2011-36 (http://www.mozilla.org/security/announce/2011/mfsa2011-36.html), MFSA 2011-37 (http://www.mozilla.org/security/announce/2011/mfsa2011-37.html), MFSA2011-38 (http://www.mozilla.org/security/announce/2011/mfsa2011-38.html), MFSA2011-39 (http://www.mozilla.org/security/announce/2011/mfsa2011-39.html), MFSA2011-40 (http://www.mozilla.org/security/announce/2011/mfsa2011-40.html), MFSA2011-41 (http://www.mozilla.org/security/announce/2011/mfsa2011-41.html), MFSA2011-42 (http://www.mozilla.org/security/announce/2011/mfsa2011-42.html), MFSA2011-43 (http://www.mozilla.org/security/announce/2011/mfsa2011-43.html), MFSA2011-44 (http://www.mozilla.org/security/announce/2011/mfsa2011-44.html), MFSA2011-45 (http://www.mozilla.org/security/announce/2011/mfsa2011-45.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA-2011-36 through MFSA-2011-45: Linux (Firefox 3.6.23) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.23&os=linux&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Linux (Firefox 7.0) (http://download.mozilla.org/?product=firefox-7.0&os=linux&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Linux (SeaMonkey 2.4) (http://download.mozilla.org/?product=seamonkey-2.4&os=linux&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Mac OS X (Firefox 7.0) (http://download.mozilla.org/?product=firefox-7.0&os=osx&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Mac OS X (Firefox 3.6.23) (http://download.mozilla.org/?product=firefox-3.6.23&os=osx&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Mac OS X (SeaMonkey 2.4) (http://download.mozilla.org/?product=seamonkey-2.4&os=osx&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Windows (Firefox 3.6.23) (http://download.mozilla.org/?product=firefox-3.6.23&os=win&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Windows (Firefox 7.0 ) (http://download.mozilla.org/?product=firefox-7.0&os=win&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Windows (SeaMonkey 2.4) (http://download.mozilla.org/?product=seamonkey-2.4&os=win&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Linux (Thunderbird 7.0) (http://download.mozilla.org/?product=thunderbird-7.0&os=linux&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Mac OS X (Thunderbird 7.0) (http://download.mozilla.org/?product=thunderbird-7.0&os=osx&lang=en-US)
MFSA-2011-36 through MFSA-2011-45: Windows (Thunderbird 7.0) (http://download.mozilla.org/?product=thunderbird-7.0&os=win&lang=en-US)

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 1.7.0.0

4 Mozilla Firefox and Thunderbird Multiple Vulnerabilities (MFSA-2011-46 through MFSA-2011-52)

| | |
|---|---|
| QID: | 119733 |
| Category: | Local |
| Associated CVEs: | CVE-2011-3647, CVE-2011-3649, CVE-2011-3648, CVE-2011-3655, CVE-2011-3653, CVE-2011-3651, CVE-2011-3650, CVE-2011-3652, CVE-2011-3654 |
| Vendor Reference: | MFSA2011-46, MFSA2011-47, MFSA2011-48, MFSA2011-49, MFSA2011-50, MFSA2011-51, MFSA2011-52 |
| Bugtraq ID: | 50591 |
| Service Modified: | 11/10/2011 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. Thunderbird is an email client.
The Mozilla Foundation has released multiple security advisories specifying vulnerabilities in Mozilla Firefox and Thunderbird. Mozilla Firefox and Thunderbird are exposed to the multiple remote vulnerabilities. See Vendor Reference for further details.
Affected Versions:
Firefox 3.x prior to 3.6.24
Thunderbird 3.x prior to 3.1.16
Firefox prior to Firefox 8
Thunderbird prior to Thunderbird 8.

IMPACT:

This vulnerability is successfully exploited, An attacker can execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in denial of service conditions.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2011-46 (http://www.mozilla.org/security/announce/2011/mfsa2011-46.html), MFSA 2011-47 (http://www.mozilla.org/security/announce/2011/mfsa2011-47.html), MFSA2011-48 (http://www.mozilla.org/security/announce/2011/mfsa2011-48.html), MFSA2011-49 (http://www.mozilla.org/security/announce/2011/mfsa2011-49.html), MFSA2011-50 (http://www.mozilla.org/security/announce/2011/mfsa2011-50.html), MFSA2011-51 (http://www.mozilla.org/security/announce/2011/mfsa2011-51.html), MFSA2011-52 (http://www.mozilla.org/security/announce/2011/mfsa2011-52.html),
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA-2011-52: Windows (Thunderbird 3.1.16) (http://download.mozilla.org/?product=thunderbird-3.1.16&os=win&lang=en-US)
MFSA-2011-52: Linux (Thunderbird 3.1.16) (http://download.mozilla.org/?product=thunderbird-3.1.16&os=linux&lang=en-US)
MFSA-2011-52: OSX (Thunderbird 3.1.16) (http://download.mozilla.org/?product=thunderbird-3.1.16&os=osx&lang=en-US)
MFSA-2011-52: Windows (Firefox 3.6.24) (http://download.mozilla.org/?product=firefox-3.6.24&os=win&lang=en-US)
MFSA-2011-52: Linux (Firefox 3.6.24) (http://download.mozilla.org/?product=firefox-3.6.24&os=linux&lang=en-US)
MFSA-2011-52: OSX (Firefox 3.6.24) (http://download.mozilla.org/?product=firefox-3.6.24&os=osx&lang=en-US)
MFSA-2011-52: Windows (Firefox 8.0) (http://download.mozilla.org/?product=firefox-8.0&os=win&lang=en-US)
MFSA-2011-52: Linux (Firefox 8.0) (http://download.mozilla.org/?product=firefox-8.0&os=linux&lang=en-US)
MFSA-2011-52: OSX (Firefox 8.0) (http://download.mozilla.org/?product=firefox-8.0&os=osx&lang=en-US)
MFSA-2011-52: Windows (thunderbird 8.0) (http://download.mozilla.org/?product=thunderbird-8.0&os=win&lang=en-US)
MFSA-2011-52: Linux (thunderbird 8.0) (http://download.mozilla.org/?product=thunderbird-8.0&os=linux&lang=en-US)
MFSA-2011-52: OSX (thunderbird 8.0) (http://download.mozilla.org/?product=thunderbird-8.0&os=osx&lang=en-US)

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 1.7.0.0

4 Mozilla Firefox, SeaMonkey and Thunderbird Security Update (MFSA-2012-04)

| | |
|---|---|
| QID: | 119920 |
| Category: | Local |
| Associated CVEs: | CVE-2011-3659 |
| Vendor Reference: | MFSA2012-04 |
| Bugtraq ID: | - |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
Mozilla products are prone to a remote code execution vulnerability caused by removed child nodes of nsDOMAttribute, which can be accessed under certain circumstances because of a premature notification of AttributeChildRemoved.
Affected Software:
Firefox versions prior to 10.0
Firefox 3.x versions prior to 3.6.26
Thunderbird versions prior to 10.0
Thunderbird 3.x versions prior 3.1.18
SeaMonkey versions prior to 2.7

IMPACT:

Successful exploitation allows attackers to execute remote code.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisory for further details: MFSA2012-04 (http://www.mozilla.org/security/announce/2012/mfsa2012-04.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2012-04: Linux (Firefox 10.0) (http://download.mozilla.org/?product=firefox-10.0&os=linux&lang=en-US)
MFSA2012-04: Linux (Firefox 3.6.26) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.26&os=linux&lang=en-US)
MFSA2012-04: Linux (thunderbird 10.0) (http://download.mozilla.org/?product=thunderbird-10.0&os=linux&lang=en-US)
MFSA2012-04: Linux (thunderbird 3.1.1) (http://download.mozilla.org/?product=thunderbird-3.1.18&os=linux&lang=en-US)
MFSA2012-04: Linux (seamonkey 2.7) (http://download.mozilla.org/?product=seamonkey-2.7&os=linux&lang=en-US)
MFSA2012-04: Mac OS X (Firefox 10.0) (http://download.mozilla.org/?product=firefox-10.0&os=osx&lang=en-US)
MFSA2012-04: Mac OS X (Firefox 3.6.26) (http://download.mozilla.org/?product=firefox-3.6.26&os=osx&lang=en-US)
MFSA2012-04: Mac OS X (thunderbird 10.0) (http://download.mozilla.org/?product=thunderbird-10.0&os=osx&lang=en-US)
MFSA2012-04: Mac OS X (thunderbird 3.1.1) (http://download.mozilla.org/?product=thunderbird-3.1.18&os=osx&lang=en-US)
MFSA2012-04: Mac OS X (seamonkey 2.7) (http://download.mozilla.org/?product=seamonkey-2.7&os=osx&lang=en-US)
MFSA2012-04: Windows (Firefox 10.0) (http://download.mozilla.org/?product=firefox-10.0&os=win&lang=en-US)
MFSA2012-04: Windows (Firefox 3.6.26) (http://download.mozilla.org/?product=firefox-3.6.26&os=win&lang=en-US)
MFSA2012-04: Windows (thunderbird 10.0) (http://download.mozilla.org/?product=thunderbird-10.0&os=win&lang=en-US)
MFSA2012-04: Windows (thunderbird 3.1.1) (http://download.mozilla.org/?product=thunderbird-3.1.18&os=win&lang=en-US)
MFSA2012-04: Windows (seamonkey 2.7) (http://download.mozilla.org/?product=seamonkey-2.7&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit
Reference: CVE-2011-3659
Description: Firefox 8/9 AttributeChildRemoved() Use-After-Free - Metasploit Ref : /modules/exploit/windows/browser/mozilla_attribchildremoved
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/browser/mozilla_attribchildremoved.rb

The Exploit-DB
Reference: CVE-2011-3659
Description: Mozilla Firefox 8/9 - 'AttributeChildRemoved()' Use-After-Free (Metasploit) - The Exploit-DB Ref : 18870
Link: http://www.exploit-db.com/exploits/18870

ExploitKits
Reference: CVE-2011-3659
Description: FIREFOX 8/9_ AttributeChildRemoved() Use-After-Free. Firefox social FIREFOX Bootstrapped Addon Social Engineering Code Execution
Link: http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html

exploitdb

Reference: CVE-2011-3659
Description: Mozilla Firefox 8/9 - 'AttributeChildRemoved()' Use-After-Free (Metasploit)
Link: https://www.exploit-db.com/exploits/18870

nvd

Reference: CVE-2011-3659
Description: Use-after-free vulnerability in Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 might allow remote attackers to execute arbitrary code via vectors related to incorrect AttributeChildRemoved notifications that affect access to removed nsDOMAttribute child nodes.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=708198

seebug

Reference: CVE-2011-3659
Description: Firefox 8/9 AttributeChildRemoved() Use-After-Free
Link: https://www.seebug.org/vuldb/ssvid-72882

saint

Reference: CVE-2011-3659
Description: Firefox AttributeChildRemoved Use After Free
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/firefox_attributechildremove_use_after_free

packetstorm

Reference: CVE-2011-3659
Description: Firefox 8/9 AttributeChildRemoved() Use-After-Free
Link: https://packetstormsecurity.com/files/112664/Firefox-8-9-AttributeChildRemoved-Use-After-Free.html

metasploit

Reference: CVE-2011-3659
Description: Firefox 8/9 AttributeChildRemoved() Use-After-Free
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2011-3659
Description: Firefox 8/9 AttributeChildRemoved() Use-After-Free
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/browser/mozilla_attribchildremoved.rb

contagio

Reference: CVE-2011-3659
Description: Phoenix Exploit Kit
Link: https://docs.google.com/spreadsheets/d/1cK7vFVn73NTsoLU487nh-XVSFu7M064RgHeDZB0a2s8/edit#gid=0

white-phosphorus

Reference: CVE-2011-3659
Description: wp_mozilla_firefox_attributechildremoved
Link: http://exploitlist.immunityinc.com/home/exploitpack/White_Phosphorus/wp_mozilla_firefox_attributechildremoved

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: ShellCode
Type: Trojan
Platform: Script

Malware ID: Generic
Type: Exploit
Platform: Script

Malware ID: Cool
Type: Exploit
Platform: Script

| | |
|---|---|
| Malware ID: | Heuristic |
| Type: | Exploit |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | CVE-2011-3659 |
| Type: | Exploit |
| Platform: | Script |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities

| | |
|---|---|
| QID: | 120197 |
| Category: | Local |
| Associated CVEs: | CVE-2011-1187, CVE-2011-3062, CVE-2012-0467, CVE-2012-0468, CVE-2012-0469, CVE-2012-0470, CVE-2012-0471, CVE-2012-0472, CVE-2012-0473, CVE-2012-0474, CVE-2012-0475, CVE-2012-0477, CVE-2012-0478, CVE-2012-0479 |
| Vendor Reference: | MFSA2012-20, MFSA2012-22, MFSA2012-23, MFSA2012-24, MFSA2012-25, MFSA2012-26, MFSA2012-27, MFSA2012-28, MFSA2012-29, MFSA2012-30, MFSA2012-31, MFSA2012-32, MFSA2012-33 |
| Bugtraq ID: | 46785,53223,53221,53220,53225,53219,53218,53231,53228,53230,53229,53227,53224 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
The Mozilla Foundation has released multiple security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird and SeaMonkey. Mozilla Firefox, Thunderbird and SeaMonkey are exposed to multiple remote vulnerabilities. See reference for further details.
Affected Versions:
Firefox prior to 12.0
Firefox ESR prior to 10.0.4
Thunderbird prior to 12.0
Thunderbird ESR prior to 10.0.4
SeaMonkey prior to 2.9

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to execute arbitrary code.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2012-20 (http://www.mozilla.org/security/announce/2012/mfsa2012-20.html), MFSA 2012-22 (http://www.mozilla.org/security/announce/2012/mfsa2012-22.html), MFSA2012-23 (http://www.mozilla.org/security/announce/2012/mfsa2012-23.html), MFSA2012-24 (http://www.mozilla.org/security/announce/2012/mfsa2012-24.html), MFSA2012-25 (http://www.mozilla.org/security/announce/2012/mfsa2012-25.html), MFSA2012-26 (http://www.mozilla.org/security/announce/2012/mfsa2012-26.html), MFSA2012-27 (http://www.mozilla.org/security/announce/2012/mfsa2012-27.html), MFSA2012-28 (http://www.mozilla.org/security/announce/2012/mfsa2012-28.html), MFSA2012-29 (http://www.mozilla.org/security/announce/2012/mfsa2012-29.html), MFSA2012-30 (http://www.mozilla.org/security/announce/2012/mfsa2012-30.html), MFSA2012-31 (http://www.mozilla.org/security/announce/2012/mfsa2012-31.html), MFSA2012-32 (http://www.mozilla.org/security/announce/2012/mfsa2012-32.html), MFSA2012-33 (http://www.mozilla.org/security/announce/2012/mfsa2012-33.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2012-33: Linux (Thunderbird 12.0) (http://download.mozilla.org/?product=thunderbird-12.0&os=linux&lang=en-US)
MFSA2012-33: Linux (Firefox 12.0) (http://download.mozilla.org/?product=firefox-12.0&os=linux&lang=en-US)
MFSA2012-33: Linux (SeaMonkey 2.9 ) (http://download.mozilla.org/?product=seamonkey-2.9&os=linux&lang=en-US)
MFSA2012-33: Linux (Firefox 10.0.4 ESR) (http://download.mozilla.org/?product=firefox-10.0.4esr&os=linux&lang=en-US)
MFSA2012-33: Linux (Thunderbird 10.0.4 ESR) (http://download.mozilla.org/?product=thunderbird-10.0.4esr&os=linux&lang=en-US)
MFSA2012-33: Windows (Thunderbird 12.0) (http://download.mozilla.org/?product=thunderbird-12.0&os=win&lang=en-US)
MFSA2012-33: Windows (Firefox 12.0) (http://download.mozilla.org/?product=firefox-12.0&os=win&lang=en-US)
MFSA2012-33: Windows (SeaMonkey 2.9 ) (http://download.mozilla.org/?product=seamonkey-2.9&os=win&lang=en-US)
MFSA2012-33: Windows (Firefox 10.0.4 ESR) (http://download.mozilla.org/?product=firefox-10.0.4esr&os=win&lang=en-US)
MFSA2012-33: Windows (Thunderbird 10.0.4 ESR) (http://download.mozilla.org/?product=thunderbird-10.0.4esr&os=win&lang=en-US)
MFSA2012-33: OSX (Thunderbird 12.0) (http://download.mozilla.org/?product=thunderbird-12.0&os=osx&lang=en-US)

MFSA2012-33: OSX (Firefox 12.0) (http://download.mozilla.org/?product=firefox-12.0&os=osx&lang=en-US)
MFSA2012-33: OSX (SeaMonkey 2.9 ) (http://download.mozilla.org/?product=seamonkey-2.9&os=osx&lang=en-US)
MFSA2012-33: OSX (Firefox 10.0.4 ESR) (http://download.mozilla.org/?product=firefox-10.0.4esr&os=osx&lang=en-US)
MFSA2012-33: OSX (Thunderbird 10.0.4 ESR) (http://download.mozilla.org/?product=thunderbird-10.0.4esr&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2011-1187
Description: Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=624621

Reference: CVE-2011-1187
Description: Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
Link: http://code.google.com/p/chromium/issues/detail?id=69187

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities (MFSA 2012-57 through MFSA 2012-73)

| | |
|---|---|
| QID: | 120451 |
| Category: | Local |
| Associated CVEs: | CVE-2012-1956, CVE-2012-1970, CVE-2012-1971, CVE-2012-1972, CVE-2012-1973, CVE-2012-1974, CVE-2012-1975, CVE-2012-1976, CVE-2012-3956, CVE-2012-3957, CVE-2012-3958, CVE-2012-3959, CVE-2012-3960, CVE-2012-3961, CVE-2012-3962, CVE-2012-3963, CVE-2012-3964, CVE-2012-3965, CVE-2012-3966, CVE-2012-3967, CVE-2012-3968, CVE-2012-3969, CVE-2012-3970, CVE-2012-3971, CVE-2012-3972, CVE-2012-3973, CVE-2012-3974, CVE-2012-3975, CVE-2012-3976, CVE-2012-3978, CVE-2012-3979, CVE-2012-3980, CVE-2012-4930 |
| Vendor Reference: | MFSA2012-57, MFSA2012-58, MFSA2012-59, MFSA2012-60, MFSA2012-61, MFSA2012-62, MFSA2012-63, MFSA2012-64, MFSA2012-65, MFSA2012-66, MFSA2012-67, MFSA2012-68, MFSA2012-69, MFSA2012-70, MFSA2012-71, MFSA2012-72, MFSA2012-73 |
| Bugtraq ID: | 55320,55341,55323,55324,55325,55321,55340,55322,55277,55276,55292,55278,55304,55311,55313,55306,55257,55260,55314,55316,55317,55318,5 |
| Service Modified: | 08/05/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
The Mozilla Foundation has released multiple security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird and SeaMonkey. Mozilla Firefox, Thunderbird and SeaMonkey are exposed to multiple remote vulnerabilities. See reference for further details.
Affected Versions:
Firefox prior to 15.0
Firefox ESR prior to 10.0.7
Thunderbird prior to 15.0
Thunderbird ESR prior to 10.0.7
SeaMonkey prior to 2.12

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to execute arbitrary code.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2012-57 (http://www.mozilla.org/security/announce/2012/mfsa2012-57.html), MFSA 2012-58 (http://www.mozilla.org/security/announce/2012/mfsa2012-58.html), MFSA2012-59 (http://www.mozilla.org/security/announce/2012/mfsa2012-59.html), MFSA2012-60 (http://www.mozilla.org/security/announce/2012/mfsa2012-60.html), MFSA2012-61

(http://www.mozilla.org/security/announce/2012/mfsa2012-61.html), MFSA2012-62 (http://www.mozilla.org/security/announce/2012/mfsa2012-62.html), MFSA2012-63 (http://www.mozilla.org/security/announce/2012/mfsa2012-63.html), MFSA2012-64 (http://www.mozilla.org/security/announce/2012/mfsa2012-64.html), MFSA2012-65 (http://www.mozilla.org/security/announce/2012/mfsa2012-65.html), MFSA2012-66 (http://www.mozilla.org/security/announce/2012/mfsa2012-66.html), MFSA2012-67 (http://www.mozilla.org/security/announce/2012/mfsa2012-67.html), MFSA2012-68 (http://www.mozilla.org/security/announce/2012/mfsa2012-68.html), MFSA2012-69 (http://www.mozilla.org/security/announce/2012/mfsa2012-69.html), MFSA2012-70 (http://www.mozilla.org/security/announce/2012/mfsa2012-70.html), MFSA2012-71 (http://www.mozilla.org/security/announce/2012/mfsa2012-71.html), MFSA2012-72 (http://www.mozilla.org/security/announce/2012/mfsa2012-72.html), MFSA2012-73 (http://www.mozilla.org/security/announce/2012/mfsa2012-73.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2012-57: OSX (Firefox 10.0.7 ESR) (http://download.mozilla.org/?product=firefox-10.0.7esr&os=osx&lang=en-US)
MFSA2012-57: OSX (Thunderbird 10.0.7 ESR) (http://download.mozilla.org/?product=thunderbird-10.0.7esr&os=osx&lang=en-US)
MFSA2012-57: OSX (SeaMonkey 2.12) (http://download.mozilla.org/?product=seamonkey-2.12&os=osx&lang=en-US)
MFSA2012-57: OSX (Firefox 15.0) (http://download.mozilla.org/?product=firefox-15.0&os=osx&lang=en-US)
MFSA2012-57: OSX (Thunderbird 15.0) (http://download.mozilla.org/?product=thunderbird-15.0&os=osx&lang=en-US)
MFSA2012-57: Windows (Thunderbird 10.0.7 ESR) (http://download.mozilla.org/?product=thunderbird-10.0.7esr&os=win&lang=en-US)
MFSA2012-57: Windows (Firefox 10.0.7 ESR) (http://download.mozilla.org/?product=firefox-10.0.7esr&os=win&lang=en-US)
MFSA2012-57: Windows (SeaMonkey 2.12) (http://download.mozilla.org/?product=seamonkey-2.12&os=win&lang=en-US)
MFSA2012-57: Windows (Firefox 15.0) (http://download.mozilla.org/?product=firefox-15.0&os=win&lang=en-US)
MFSA2012-57: Windows (Thunderbird 15.0) (http://download.mozilla.org/?product=thunderbird-15.0&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2012-3961
Description: Use-after-free vulnerability in the RangeData implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=771873

Reference: CVE-2012-3967
Description: The WebGL implementation in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 on Linux, when a large number of sampler uniforms are used, does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via a crafted web site.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=777028

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/SeaMonkey/Thunderbird Multiple Vulnerabilities (MFSA 2012-91 through MFSA 2012-106)

| | |
|---|---|
| QID: | 120696 |
| Category: | Local |
| Associated CVEs: | CVE-2012-4201, CVE-2012-4202, CVE-2012-4203, CVE-2012-4204, CVE-2012-4205, CVE-2012-4206, CVE-2012-4207, CVE-2012-4208, CVE-2012-4209, CVE-2012-4210, CVE-2012-4212, CVE-2012-4213, CVE-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-4217, CVE-2012-4218, CVE-2012-5829, CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5836, CVE-2012-5837, CVE-2012-5838, CVE-2012-5839, CVE-2012-5840, CVE-2012-5841, CVE-2012-5842, CVE-2012-5843 |
| Vendor Reference: | MFSA2012-100, MFSA2012-101, MFSA2012-102, MFSA2012-103, MFSA2012-104, MFSA2012-105, MFSA2012-106, MFSA2012-91, MFSA2012-92, MFSA2012-93, MFSA2012-94, MFSA2012-95, MFSA2012-96, MFSA2012-97, MFSA2012-98, MFSA2012-99 |
| Bugtraq ID: | 56636,56642,56643,56616,56645,56644,56637,56635,56631,56611,56618,56614,56623,56621,56632,56627,56629,56646,56630,56638,56628,56633,5 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.

Mozilla has fixed a number of issues related to the Location object in order to enhance overall security.
Affected Versions:
Firefox prior to 17
Firefox ESR prior to 10.0.11
Thunderbird prior to 17
Thunderbird ESR prior to 10.0.11
SeaMonkey prior to 2.14

IMPACT:

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

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2012-91 (http://www.mozilla.org/security/announce/2012/mfsa2012-91.html), MFSA 2012-92 (http://www.mozilla.org/security/announce/2012/mfsa2012-92.html), MFSA2012-93 (http://www.mozilla.org/security/announce/2012/mfsa2012-93.html), MFSA2012-94 (http://www.mozilla.org/security/announce/2012/mfsa2012-94.html), MFSA2012-95 (http://www.mozilla.org/security/announce/2012/mfsa2012-95.html), MFSA2012-96 (http://www.mozilla.org/security/announce/2012/mfsa2012-96.html), MFSA2012-97 (http://www.mozilla.org/security/announce/2012/mfsa2012-97.html), MFSA2012-98 (http://www.mozilla.org/security/announce/2012/mfsa2012-98.html), MFSA2012-99 (http://www.mozilla.org/security/announce/2012/mfsa2012-99.html), MFSA2012-100 (http://www.mozilla.org/security/announce/2012/mfsa2012-100.html), MFSA2012-101 (http://www.mozilla.org/security/announce/2012/mfsa2012-101.html), MFSA2012-102 (http://www.mozilla.org/security/announce/2012/mfsa2012-102.html), MFSA2012-103 (http://www.mozilla.org/security/announce/2012/mfsa2012-103.html), MFSA2012-104 (http://www.mozilla.org/security/announce/2012/mfsa2012-104.html), MFSA2012-105 (http://www.mozilla.org/security/announce/2012/mfsa2012-105.html), MFSA2012-106 (http://www.mozilla.org/security/announce/2012/mfsa2012-106.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 17.0: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0/mac/en-US/Firefox%2017.0.dmg)
Firefox 17.0: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0/win32/en-US/Firefox%20Setup%2017.0.exe)
Thunderbird 17.0: Windows (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0/win32/en-US/Thunderbird%20Setup%2017.0.exe)
Thunderbird 17.0: Mac (http://download-origin.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0/mac/en-US/Thunderbird%2017.0.dmg)
SeaMonkey: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.14/win32/en-US/SeaMonkey%20Setup%202.14.exe)
SeaMonkey: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.14/mac/en-US/SeaMonkey%202.14.dmg)
Firefox ESR 10.0.11: Mac (http://download.mozilla.org/?product=firefox-10.0.11esr&os=osx&lang=en-US)
Firefox ESR 10.0.11: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/10.0.11esr/win32/en-US/Firefox%20Setup%2010.0.11esr.exe)
Thunderbird  ESR 10.0.11: Mac (http://download.mozilla.org/?product=thunderbird-10.0.11esr&os=osx&lang=en-US)
Thunderbird  ESR 10.0.11: Windows (http://download.mozilla.org/?product=thunderbird-10.0.11esr&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2012-5829
Description: Heap-based buffer overflow in the nsWindow::OnExposeEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=792305

Reference: CVE-2012-5830
Description: Use-after-free vulnerability in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 on Mac OS X allows remote attackers to execute arbitrary code via an HTML document.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=775228

Reference: CVE-2012-5835
Description: Integer overflow in the WebGL subsystem in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (invalid write operation) via crafted data.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=790879

Reference: CVE-2012-5838
Description: The copyTexImage2D implementation in the WebGL subsystem in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via large image dimensions.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=802778

Reference: CVE-2012-5840
Description: Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4214.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=805287

Reference: CVE-2012-4213
Description: Use-after-free vulnerability in the nsEditor::FindNextLeafNode function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=795708

Reference: CVE-2012-4214
Description: Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-5840.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=795804

Reference: CVE-2012-4215
Description: Use-after-free vulnerability in the nsPlaintextEditor::FireClipboardEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=798677

Reference: CVE-2012-4216
Description: Use-after-free vulnerability in the gfxFont::GetFontEntry function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=798853

Reference: CVE-2012-4217
Description: Use-after-free vulnerability in the nsViewManager::ProcessPendingUpdates function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=802902

Reference: CVE-2012-5843
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=797163

Reference: CVE-2012-5843
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=791601

Reference: CVE-2012-5843
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=788822

Reference: CVE-2012-5843
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=781859

Reference: CVE-2012-4201
Description: The evalInSandbox implementation in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 uses an incorrect context during the handling of JavaScript code that sets the location.href property, which allows remote attackers to conduct cross-site scripting (XSS) attacks or read arbitrary files by leveraging a sandboxed add-on.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=747607

Reference: CVE-2012-4204
Description: The str_unescape function in the JavaScript engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=778603

Reference: CVE-2012-4207
Description: The HZ-GB-2312 character-set implementation in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0,

Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 does not properly handle a ~ (tilde) character in proximity to a chunk delimiter, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted document.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=801681

packetstorm

Reference: CVE-2012-5835

Description: Mozilla Firefox WebGL Proof Of Concept

Link: https://packetstormsecurity.com/files/141118/Mozilla-Firefox-WebGL-Proof-Of-Concept.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/SeaMonkey/Thunderbird Multiple Vulnerabilities (MFSA 2013-30 through MFSA 2013-40)

| | |
|---|---|
| QID: | 121046 |
| Category: | Local |
| Associated CVEs: | CVE-2013-0788, CVE-2013-0789, CVE-2013-0792, CVE-2013-0793, CVE-2013-0794, CVE-2013-0795, CVE-2013-0796, CVE-2013-0797, CVE-2013-0799, CVE-2013-0800 |
| Vendor Reference: | mfsa2013-30.html, mfsa2013-31.html, mfsa2013-32.html, mfsa2013-33.html, mfsa2013-34.html, mfsa2013-35.html, mfsa2013-36.html, mfsa2013-37.html, mfsa2013-38.html, mfsa2013-39.html, mfsa2013-40.html |
| Bugtraq ID: | 58821,58824,58825,58826,58827,58828,58835,58836,58837 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird and SeaMonkey:
1) Some unspecified errors can be exploited to cause memory corruption. No further information is currently available.
2) Some more unspecified errors can be exploited to cause memory corruption. No further information is currently available.
3) An out-of-bounds write error when rendering exists in the Cairo library.
4) An unspecified error in the Mozilla Maintenance Service can be exploited to cause a buffer overflow via arbitrary arguments and execute arbitrary code with the privileges of the service.
5) The application loads a certain library in an insecure manner, which can be exploited to load arbitrary libraries.
6) An error in WebGL rendering within the Mesa graphics driver can be exploited to dereference unallocated memory.
7) An error when cloning a node via the "cloneNode()" method can be exploited to bypass System Only Wrappers (SOW) and the same origin policy.
8) An error when handling the origin of tab-modal dialog boxes in combination with browser navigation can be exploited to display a dialog while displaying an arbitrary page.
9) An error related to a baseURI of a page within the history can be exploited to spoof the URL displayed in the addressbar while displaying a different page and execute script code.
10) An error when handling grayscale PNG image rendering using certain color profiles can be exploited to corrupt memory via a specially crafted PNG image.
Affected Versions:
Firefox prior to 20.0
Firefox ESR prior to17.0.5
Thunderbird prior to 17.0.5
Thunderbird ESR prior to 17.0.5
SeaMonkey prior to 2.17

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to mfsa2013-30 (http://www.mozilla.org/security/announce/2013/mfsa2013-30.html), mfsa2013-31 (http://www.mozilla.org/security/announce/2013/mfsa2013-31.html), mfsa2013-32 (http://www.mozilla.org/security/announce/2013/mfsa2013-32.html), mfsa2013-33 (http://www.mozilla.org/security/announce/2013/mfsa2013-33.html), mfsa2013-34 (http://www.mozilla.org/security/announce/2013/mfsa2013-34.html), mfsa2013-35 (http://www.mozilla.org/security/announce/2013/mfsa2013-35.html), mfsa2013-36 (http://www.mozilla.org/security/announce/2013/mfsa2013-36.html), mfsa2013-37 (http://www.mozilla.org/security/announce/2013/mfsa2013-37.html), mfsa2013-38 (http://www.mozilla.org/security/announce/2013/mfsa2013-38.html), mfsa2013-39 (http://www.mozilla.org/security/announce/2013/mfsa2013-39.html), mfsa2013-40 (http://www.mozilla.org/security/announce/2013/mfsa2013-40.html) for further information.
Patch:

Following are links for downloading patches to fix the vulnerabilities:
Firefox 17.0.5esr: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.5esr/mac/en-US/Firefox%2017.0.5esr.dmg)
Firefox 17.0.5esr: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.5esr/win32/en-US/Firefox%20Setup%2017.0.5esr.exe)
Firefox 20: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/20.0/mac/en-US/Firefox%2020.0.dmg)
Firefox 20: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/20.0/win32/en-US/Firefox%20Setup%2020.0.exe)
SeaMonkey 2.17: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.17/mac/en-US/SeaMonkey%202.17.dmg)
SeaMonkey 2.17: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/seamonkey/releases/2.17/win32/en-US/SeaMonkey%20Setup%202.17.exe)
Thunderbird 17.0.5: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.5/mac/en-US/Thunderbird%2017.0.5.dmg)
Thunderbird 17.0.5: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.5/win32/en-US/Thunderbird%20Setup%2017.0.5.exe)
Thunderbird 17.0.5esr: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.5esr/mac/en-US/Thunderbird%2017.0.5esr.dmg)
Thunderbird 17.0.5esr: Windows
(http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.5esr/win32/en-US/Thunderbird%20Setup%2017.0.5esr.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2013-0796
Description: The WebGL subsystem in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 on Linux does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (free of unallocated memory) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=827106

Reference: CVE-2013-0796
Description: The WebGL subsystem in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 on Linux does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (free of unallocated memory) via unspecified vectors.
Link: http://www.mozilla.org/security/announce/2013/mfsa2013-35.html

Reference: CVE-2013-0796
Description: The WebGL subsystem in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, and SeaMonkey before 2.17 on Linux does not properly interact with Mesa drivers, which allows remote attackers to execute arbitrary code or cause a denial of service (free of unallocated memory) via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=838413

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox/Thunderbird Multiple Vulnerabilities (MFSA 2013-41 through MFSA 2013-48)

| | |
|---|---|
| QID: | 121178 |
| Category: | Local |
| Associated CVEs: | CVE-2013-0801, CVE-2013-1669, CVE-2013-1670, CVE-2013-1671, CVE-2013-1672, CVE-2013-1673, CVE-2013-1942, CVE-2013-1674, CVE-2013-1675, CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681 |
| Vendor Reference: | mfsa2013-41.html, mfsa2013-42.html, mfsa2013-43.html, mfsa2013-44.html, mfsa2013-45.html, mfsa2013-46.html, mfsa2013-47.html, mfsa2013-48.html |
| Bugtraq ID: | 59030,59855,59870,59865,59859,59858,59863,59868,59864,59860,59861,59862 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird and SeaMonkey:
1) Miscellaneous memory safety hazards
2) Privileged access for content level constructor
3) File input control has access to full path
4) Local privilege escalation through Mozilla Maintenance Service

5) Mozilla Updater fails to update some Windows Registry entries
6) Use-after-free with video and onresize event
7) Uninitialized functions in DOMSVGZoomEvent
8) Memory corruption found using Address Sanitizer
Affected Versions:
Firefox prior to 21.0
Firefox ESR prior to 17.0.6
Thunderbird prior to 17.0.6
Thunderbird ESR  prior to 17.0.6

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to mfsa2013-41 (http://www.mozilla.org/security/announce/2013/mfsa2013-41.html), mfsa2013-42 (http://www.mozilla.org/security/announce/2013/mfsa2013-42.html), mfsa2013-43 (http://www.mozilla.org/security/announce/2013/mfsa2013-43.html), mfsa2013-44 (http://www.mozilla.org/security/announce/2013/mfsa2013-44.html), mfsa2013-45 (http://www.mozilla.org/security/announce/2013/mfsa2013-45.html), mfsa2013-46 (http://www.mozilla.org/security/announce/2013/mfsa2013-46.html), mfsa2013-47 (http://www.mozilla.org/security/announce/2013/mfsa2013-47.html), mfsa2013-48 (http://www.mozilla.org/security/announce/2013/mfsa2013-48.html) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 21.0: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/21.0/win32/en-US/Firefox%20Setup%2021.0.exe)
Firefox 21.0: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/21.0/mac/en-US/Firefox%2021.0.dmg)
Firefox ESR 17.0.6: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.6esr/mac/en-US/Firefox%2017.0.6esr.dmg)
Firefox ESR 17.0.6: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/17.0.6esr/win32/en-US/Firefox%20Setup%2017.0.6esr.exe)
Thunderbird 17.0.6: Mac (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.6/mac/en-US/Thunderbird%2017.0.6.dmg)
Thunderbird 17.0.6: Windows (http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/17.0.6/win32/en-US/Thunderbird%20Setup%2017.0.6.exe)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2013-1942
Description: jPlayer - 'Jplayer.swf' Script Cross-Site Scripting - The Exploit-DB Ref : 38460
Link: http://www.exploit-db.com/exploits/38460

Reference: CVE-2013-1670
Description: Mozilla Firefox - toString console.time Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 34363
Link: http://www.exploit-db.com/exploits/34363

exploitdb

Reference: CVE-2013-1670
Description: Mozilla Firefox - toString console.time Privileged JavaScript Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/34363

Reference: CVE-2013-1942
Description: jPlayer - 'Jplayer.swf' Script Cross-Site Scripting
Link: https://www.exploit-db.com/exploits/38460

nvd

Reference: CVE-2013-1942
Description: Multiple cross-site scripting (XSS) vulnerabilities in actionscript/Jplayer.as in the Flash SWF component (jplayer.swf) in jPlayer before 2.2.20, as used in ownCloud Server before 5.0.4 and other products, allow remote attackers to inject arbitrary web script or HTML via the (1) jQuery or (2) id parameters, as demonstrated using document.write in the jQuery parameter, a different vulnerability than CVE-2013-2022 and CVE-2013-2023.
Link: https://github.com/happyworm/jPlayer/commit/e8ca190f7f972a6a421cb95f09e138720e40ed6d

packetstorm

Reference: CVE-2013-1670
Description: Firefox toString console.time Privileged Javascript Injection
Link: https://packetstormsecurity.com/files/127915/Firefox-toString-console.time-Privileged-Javascript-Injection.html

0day.today

Reference: CVE-2013-1670
Description: Firefox toString console.time Privileged Javascript Injection Exploit
Link: https://0day.today/exploit/22528

cisa-kev

Reference: CVE-2013-1675
Description: Mozilla Firefox Information Disclosure Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2012-88 through MFSA 2012-89)

| | |
|---|---|
| QID: | 121254 |
| Category: | Local |
| Associated CVEs: | CVE-2012-4193, CVE-2012-4190, CVE-2012-4192, CVE-2012-4191 |
| Vendor Reference: | MFSA2012-88, MFSA2012-89 |
| Bugtraq ID: | 56155 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
1) The protected "location" object is accessible by other domain objects..
2) An unspecified error within the "FT2FontEntry::CreateFontEntry()" function.
3) An unspecified error within the "mozilla::net::FailDelayManager::Lookup()" function.
4) An error within security wrappers does not unwrap the "defaultValue" properly.
Affected Versions:
Firefox prior to 16.0.1
Firefox prior to ESR 10.0.9
Thunderbird prior to 16.0.1
Thunderbird prior to ESR 10.0.9
SeaMonkey prior to 2.13.1

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to mfsa2012-88 (http://www.mozilla.org/security/announce/2012/mfsa2012-88.html), mfsa2012-89 (http://www.mozilla.org/security/announce/2012/mfsa2012-89.html) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2012-89: OSX (Firefox 16.0.1) (http://download.mozilla.org/?product=firefox-16.0.1&os=osx&lang=en-US)
MFSA2012-89: OSX (Firefox ESR 10.0.9) (http://download.mozilla.org/?product=firefox-10.0.9esr&os=osx&lang=en-US)
MFSA2012-89: OSX (Thunderbird 16.0.1) (http://download.mozilla.org/?product=thunderbird-16.0.1&os=osx&lang=en-US)
MFSA2012-89: OSX (Thunderbird ESR 10.0.9) (http://download.mozilla.org/?product=thunderbird-10.0.9esr&os=osx&lang=en-US)
MFSA2012-89: OSX (SeaMonkey 2.13.1) (http://download.mozilla.org/?product=seamonkey-2.13.1&os=osx&lang=en-US)
MFSA2012-89: Windows (Firefox 16.0.1) (http://download.mozilla.org/?product=firefox-16.0.1&os=win&lang=en-US)
MFSA2012-89: Windows (Firefox ESR 10.0.9) (http://download.mozilla.org/?product=firefox-10.0.9esr&os=win&lang=en-US)
MFSA2012-89: Windows (Thunderbird 16.0.1) (http://download.mozilla.org/?product=thunderbird-16.0.1&os=win&lang=en-US)
MFSA2012-89: Windows (Thunderbird ESR 10.0.9) (http://download.mozilla.org/?product=thunderbird-10.0.9esr&os=win&lang=en-US)
MFSA2012-89: Windows (SeaMonkey 2.13.1) (http://download.mozilla.org/?product=seamonkey-2.13.1&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2012-4192
Description: Mozilla Firefox 16.0, Thunderbird 16.0, and SeaMonkey 2.13 allow remote attackers to bypass the Same Origin Policy and read the properties of a

Location object via a crafted web site, a related issue to CVE-2012-4193.

Link: http://www.thespanner.co.uk/2012/10/10/firefox-knows-what-your-friends-did-last-summer/

Reference: CVE-2012-4193

Description: Mozilla Firefox before 16.0.1, Firefox ESR 10.x before 10.0.9, Thunderbird before 16.0.1, Thunderbird ESR 10.x before 10.0.9, and SeaMonkey before 2.13.1 omit a security check in the defaultValue function during the unwrapping of security wrappers, which allows remote attackers to bypass the Same Origin Policy and read the properties of a Location object, or execute arbitrary JavaScript code, via a crafted web site.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=720619

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2013-76 through MFSA 2013-92)

| | |
|---|---|
| QID: | 121466 |
| Category: | Local |
| Associated CVEs: | CVE-2013-1737, CVE-2013-1736, CVE-2013-1735, CVE-2013-1732, CVE-2013-1730, CVE-2013-1726, CVE-2013-1725, CVE-2013-1722, CVE-2013-1719, CVE-2013-1718, CVE-2013-1738, CVE-2013-1728, CVE-2013-1724, CVE-2013-1723, CVE-2013-1720, CVE-2013-1731, CVE-2013-1729, CVE-2013-1727, CVE-2013-1721 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 62463,62462,62465,62460,62472,62464,62467,62468,62473,62469,62479,62478,62475,62466 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
GC hazard with default compartments and frame chain restorationUser-defined properties on DOM proxies get the wrong "this" objectMemory corruption involving scrollingBuffer overflow with multi-column, lists, and floatscompartment mismatch re-attaching XBL-backed nodesShared object library loading from writable locationWebGL Information disclosure through OS X NVIDIA graphic driversUninitialized data in IonMonkeySame-origin bypass through symbolic linksMozilla Updater does not lock MAR file after signature verificationCalling scope for new Javascript objects can lead to memory corruptionUse-after-free with select elementNativeKey continues handling key messages after widget is destroyedUse-after-free in Animation Manager during stylesheet cloningInteger overflow in ANGLE libraryImproper state in HTML5 Tree Builder with templatesMiscellaneous memory safety hazards
Affected Versions:
All Mozilla Firefox versions prior to version 24.0
All Mozilla Firefox ESR version prior to 17.0.9
All Mozilla Thunderbird version prior to 24.0
All Mozilla Thunderbird ESR version prior to 17.0.9
All Mozilla SeaMonkey versions prior to 2.21

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2013-1727

Description: Mozilla Firefox 9.0.1 - Same Origin Policy Security Bypass - The Exploit-DB Ref : 38766

Link: http://www.exploit-db.com/exploits/38766

exploitdb
Reference: CVE-2013-1727
Description: Mozilla Firefox 9.0.1 - Same Origin Policy Security Bypass
Link: https://www.exploit-db.com/exploits/38766

packetstorm
Reference: CVE-2013-1727
Description: Firefox For Android Same-Origin Bypass
Link: https://packetstormsecurity.com/files/123449/Firefox-For-Android-Same-Origin-Bypass.html

0day.today
Reference: CVE-2013-1727
Description: Firefox For Android Same-Origin Bypass
Link: https://0day.today/exploit/21312

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: Generic
Type: Trojan
Platform: ByteCode

Malware ID: Generic
Type: Exploit
Platform: ByteCode

Malware ID: CVE-2012-1723
Type: Exploit
Platform: ByteCode

Malware ID: CVE-2013-1493
Type: Exploit
Platform: ByteCode

Malware ID: CVE-2013-1723
Type: Exploit
Platform: ByteCode

Malware ID: CVE-2013-2423
Type: Exploit
Platform: ByteCode

Malware ID: CVE-2013-0422
Type: Exploit
Platform: ByteCode

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2013-93 through MFSA 2013-102)

QID: 121564
Category: Local

| | |
|---|---|
| Associated CVEs: | CVE-2013-5590, CVE-2013-5591, CVE-2013-5592, CVE-2013-5593, CVE-2013-5594, CVE-2013-5595, CVE-2013-5596, CVE-2013-5597, CVE-2013-5598, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604, CVE-2013-1739 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 63422,63428,63424,63423,63415,63430,63427,63421,63405,62966 |
| Service Modified: | 11/04/2013 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
- A use-after free error exists when interacting with HTML document templates.- An error when handling workers with direct proxies within the JavaScript engine can be exploited to cause memory corruption.- Multiple use-after-free errors exist related to missing strong references in the browsing engine.- Security bypass of PDF.js checks using iframes- A use-after-free error exists when handling state change events during update of the offline cache.- A race condition error when handling cycle collected image objects can be exploited to cause a release of a cycle collected image object within a wrong thread via a specially crafted large page.- ISome errors when handling memory allocations in the JavaScript engine can be exploited to cause buffer overflows.- An error when handling uninitialised data during Extensible Stylesheet Language Transformation (XSLT) processing can be exploited to cause an access violation.- An unspecified error can be exploited to spoof the address bar by placing arbitrary HTML content within "select" elements in arbitrary locations.- Miscellaneous memory safety hazards.
Affected Versions:
All Mozilla Firefox versions prior to version 25.0
All Mozilla Firefox ESR version prior to 24.1
All Mozilla Firefox ESR version prior to 17.0.10
All Mozilla Thunderbird version prior to 24.1
All Mozilla Thunderbird ESR version prior to 17.0.10
All Mozilla SeaMonkey versions prior to 2.22

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.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)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 4 Mozilla Firefox / SeaMonkey NSS Multiple Vulnerabilities (MFSA-2013-103)

| | |
|---|---|
| QID: | 121591 |
| Category: | Local |
| Associated CVEs: | CVE-2013-5605, CVE-2013-5606, CVE-2013-5607, CVE-2013-1741, CVE-2013-2566 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 63738,58796,63736,63737,63802 |
| Service Modified: | 08/16/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox and SeaMonkey:
- Integer truncation error in certificate parsing
- Null Cipher buffer overflow
- CERT_VerifyCert can SECSuccess for bad certificates leading to memoryset overrun
- Plaintext recovery vulnerability in RC4 used in TLS
- Unspecified integer-overflow vulnerability
Affected Versions:
All Firefox versions prior to 25.0.1
All Firefox ESR versions prior to 24.1.1
All Firefox ESR versions prior to 17.0.11
All Seamonkey versions prior to 2.22.1.

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

metasploit

Reference: CVE-2013-2566
Description: SSL/TLS Version Detection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/ssl/ssl_version.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2013-104 through MFSA 2013-117)

| | |
|---|---|
| QID: | 121630 |
| Category: | Local |
| Associated CVEs: | CVE-2013-5609, CVE-2013-5610, CVE-2013-5611, CVE-2013-5612, CVE-2013-5613, CVE-2013-5614, CVE-2013-5615, CVE-2013-5616, CVE-2013-5618, CVE-2013-5619, CVE-2013-6629, CVE-2013-6630, CVE-2013-6671, CVE-2013-6672, CVE-2013-6673 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 64205,64212,64210,64213,63676 |
| Service Modified: | 08/05/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey:
- Mis-issued ANSSI/DCSSI certificate
- JPEG information leak
- GetElementIC typed array stubs can be generated outside observed typesets

- Use-after-free in synthetic mouse movement
- Trust settings for built-in roots ignored during EV certificate validation
- Segmentation violation when replacing ordered list elements
- Potential overflow in JavaScript binary search algorithms
- Use-after-free during Table Editing
- Use-after-free in event listeners
- Sandbox restrictions not applied to nested object elements
- Character encoding cross-origin XSS attack
- Application Installation doorhanger persists on navigation
- Miscellaneous memory safety hazards (rv:26.0 / rv:24.2)

Affected Versions:
All Mozilla Firefox versions prior to version 26.0
All Mozilla Firefox ESR version prior to 24.2
All Mozilla Thunderbird version prior to 24.2
All Mozilla SeaMonkey versions prior to 2.23

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2013-5609
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=905382

Reference: CVE-2013-5609
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=937582

Reference: CVE-2013-5609
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=886850

Reference: CVE-2013-5613
Description: Use-after-free vulnerability in the PresShell::DispatchSynthMouseMove function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving synthetic mouse movement, related to the RestyleManager::GetHoverGeneration function.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=932449

Reference: CVE-2013-5613
Description: Use-after-free vulnerability in the PresShell::DispatchSynthMouseMove function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving synthetic mouse movement, related to the RestyleManager::GetHoverGeneration function.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=930381

Reference: CVE-2013-5615
Description: The JavaScript implementation in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 does not properly enforce certain typeset restrictions on the generation of GetElementIC typed array stubs, which has unspecified impact and remote attack vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=929261

Reference: CVE-2013-5616
Description: Use-after-free vulnerability in the nsEventListenerManager::HandleEventSubType function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to mListeners event listeners.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=938341

Reference: CVE-2013-5618
Description: Use-after-free vulnerability in the nsNodeUtils::LastRelease function in the table-editing user interface in the editor component in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code by triggering improper garbage collection.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=926361

Reference: CVE-2013-6671
Description: The nsGfxScrollFrameInner::IsLTR function in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allows remote attackers to execute arbitrary code via crafted use of JavaScript code for ordered list elements.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=930281

Reference: CVE-2013-6673
Description: Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 do not recognize a user's removal of trust from an EV X.509 certificate, which makes it easier for man-in-the-middle attackers to spoof SSL servers in opportunistic circumstances via a valid certificate that is unacceptable to the user.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=917380

Reference: CVE-2013-5609
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=922009

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2014-01 through MFSA 2014-13)

| | |
|---|---|
| QID: | 121773 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1477, CVE-2014-1478, CVE-2014-1479, CVE-2014-1480, CVE-2014-1482, CVE-2014-1483, CVE-2014-1484, CVE-2014-1485, CVE-2014-1486, CVE-2014-1487, CVE-2014-1489, CVE-2014-1488, CVE-2014-1491, CVE-2014-1481, CVE-2014-1495 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 65332,65316,65323,65322,65334,65317,65330,65324,65320,65321,65331,65329,65326,65328 |
| Service Modified: | 08/04/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
All Mozilla Firefox versions prior to version 27.0
All Mozilla Firefox ESR version prior to 24.3
All Mozilla Thunderbird version prior to 24.3
All Mozilla SeaMonkey versions prior to 2.24

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=950438

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=936808

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=945939

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=950000

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=937132

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=937697

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=945334

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=921470

Reference: CVE-2014-1477
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=953114

Reference: CVE-2014-1477

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=925896

Reference: CVE-2014-1477

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=951366

Reference: CVE-2014-1479

Description: The System Only Wrapper (SOW) implementation in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 does not prevent certain cloning operations, which allows remote attackers to bypass intended restrictions on XUL content via vectors involving XBL content scopes.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=911864

Reference: CVE-2014-1481

Description: Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to bypass intended restrictions on window objects by leveraging inconsistency in native getter methods across different JavaScript engines.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=936056

Reference: CVE-2014-1482

Description: RasterImage.cpp in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 does not prevent access to discarded data, which allows remote attackers to execute arbitrary code or cause a denial of service (incorrect write operations) via crafted image data, as demonstrated by Goo Create.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=943803

Reference: CVE-2014-1487

Description: The Web workers implementation in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allows remote attackers to bypass the Same Origin Policy and obtain sensitive authentication information via vectors involving error messages.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=947592

Reference: CVE-2014-1491

Description: Mozilla Network Security Services (NSS) before 3.15.4, as used in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, SeaMonkey before 2.24, and other products, does not properly restrict public values in Diffie-Hellman key exchanges, which makes it easier for remote attackers to bypass cryptographic protection mechanisms in ticket handling by leveraging use of a certain value.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=934545

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2014-15 through MFSA 2014-20 ,22,23 and MFSA 2014 -26 through MFSA 2014-32)

| | |
|---|---|
| QID: | 121856 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1493, CVE-2014-1494, CVE-2014-1496, CVE-2014-1497, CVE-2014-1498, CVE-2014-1499, CVE-2014-1500, CVE-2014-1502, CVE-2014-1504, CVE-2014-1505, CVE-2014-1508, CVE-2014-1509, CVE-2014-1510, CVE-2014-1511, CVE-2014-1512, CVE-2014-1513, CVE-2014-1514 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 66412,66423,66418,66426,66425,66206,66207,66209,66203,66240 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox, Thunderbird and SeaMonkey:
- Out-of-bounds write vulnerability through TypedArrayObject after neutering
- Out-of-bounds read/write vulnerability through neutering ArrayBuffer objects
- Use-after-free vulnerability in TypeObject - Privilege escalation vulnerability using WebIDL-implemented APIs
- SVG filters information disclosure vulnerability through feDisplacementMap
- Memory corruption vulnerability in Cairo during PDF font rendering
- Information disclosure vulnerability through polygon rendering in MathML
- Out of bounds read vulnerability during WAV file decoding
- Files extracted during updates are not always read only
- Miscellaneous memory safety hazards
- Content Security Policy for data: documents not preserved by session restore
- WebGL content injection vulnerability from one domain to rendering in another
- onbeforeunload and Javascript navigation DOS vulnerability
- Spoofing attack on WebRTC permission prompt
- crypto.generateCRMFRequest does not validate type of key
Affected Versions:
All Mozilla Firefox versions prior to version 28.0
All Mozilla Firefox ESR version prior to 24.4
All Mozilla Thunderbird version prior to 24.4
All Mozilla SeaMonkey versions prior to 2.25

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2014-1510
Description: Firefox WebIDL Privileged Javascript Injection - Metasploit Ref : /modules/auxiliary/admin/http/sophos_wpa_traversal
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_webidl_injection.rb

Reference: CVE-2014-1511
Description: Firefox WebIDL Privileged Javascript Injection - Metasploit Ref : /modules/auxiliary/admin/http/sophos_wpa_traversal
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_webidl_injection.rb

Reference: CVE-2014-1510
Description: Firefox WebIDL Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_webidl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_webidl_injection.rb

Reference: CVE-2014-1511
Description: Firefox WebIDL Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_webidl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_webidl_injection.rb

The Exploit-DB

Reference: CVE-2014-1510
Description: Mozilla Firefox - WebIDL Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 34448
Link: http://www.exploit-db.com/exploits/34448

Reference: CVE-2014-1511
Description: Mozilla Firefox - WebIDL Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 34448
Link: http://www.exploit-db.com/exploits/34448

exploitdb

Reference: CVE-2014-1510
Description: Mozilla Firefox - WebIDL Privileged JavaScript Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/34448

Reference: CVE-2014-1511
Description: Mozilla Firefox - WebIDL Privileged JavaScript Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/34448

nvd

Reference: CVE-2014-1510
Description: The Web IDL implementation in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to execute arbitrary JavaScript code with chrome privileges by using an IDL fragment to trigger a window.open call.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=982906

Reference: CVE-2014-1511
Description: Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to bypass the popup blocker via unspecified vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=982909

Reference: CVE-2014-1512
Description: Use-after-free vulnerability in the TypeObject class in the JavaScript engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to execute arbitrary code by triggering extensive memory consumption while garbage collection is occurring, as demonstrated by improper handling of BumpChunk objects.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=982957

Reference: CVE-2014-1513
Description: TypedArrayObject.cpp in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 does not prevent a zero-length transition during use of an ArrayBuffer object, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based out-of-bounds write or read) via a crafted web site.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=982974

Reference: CVE-2014-1514
Description: vmtypedarrayobject.cpp in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 does not validate the length of the destination array before a copy operation, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write and application crash) by triggering incorrect use of the TypedArrayObject class.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=983344

Reference: CVE-2014-1493
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=967341

Reference: CVE-2014-1493
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=963974

Reference: CVE-2014-1493
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=965982

Reference: CVE-2014-1493
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=977538

Reference: CVE-2014-1493
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly

execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=958867

Reference: CVE-2014-1493

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=896268

Reference: CVE-2014-1493

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=960145

Reference: CVE-2014-1496

Description: Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 might allow local users to gain privileges by modifying the extracted Mar contents during an update.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=925747

Reference: CVE-2014-1497

Description: The mozilla::WaveReader::DecodeAudioData function in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive information from process heap memory, cause a denial of service (out-of-bounds read and application crash), or possibly have unspecified other impact via a crafted WAV file.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=966311

Reference: CVE-2014-1505

Description: The SVG filter implementation in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive displacement-correlation information, and possibly bypass the Same Origin Policy and read text from a different domain, via a timing attack involving feDisplacementMap elements, a related issue to CVE-2013-1693.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=941887

Reference: CVE-2014-1508

Description: The libxul.so!gfxContext::Polygon function in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to obtain sensitive information from process memory, cause a denial of service (out-of-bounds read and application crash), or possibly bypass the Same Origin Policy via vectors involving MathML polygon rendering.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=963198

Reference: CVE-2014-1509

Description: Buffer overflow in the _cairo_truetype_index_to_ucs4 function in cairo, as used in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25, allows remote attackers to execute arbitrary code via a crafted extension that renders fonts in a PDF document.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=966021

packetstorm

Reference: CVE-2014-1510

Description: Firefox WebIDL Privileged Javascript Injection

Link: https://packetstormsecurity.com/files/128022/Firefox-WebIDL-Privileged-Javascript-Injection.html

Reference: CVE-2014-1511

Description: Firefox WebIDL Privileged Javascript Injection

Link: https://packetstormsecurity.com/files/128022/Firefox-WebIDL-Privileged-Javascript-Injection.html

metasploit

Reference: CVE-2014-1510

Description: Firefox WebIDL Privileged Javascript Injection

Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2014-1511

Description: Firefox WebIDL Privileged Javascript Injection

Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2014-1511

Description: Firefox WebIDL Privileged Javascript Injection

Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_webidl_injection.rb

Reference: CVE-2014-1510
Description: Firefox WebIDL Privileged Javascript Injection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_webidl_injection.rb

0day.today
Reference: CVE-2014-1510
Description: Firefox WebIDL Privileged Javascript Injection Exploit
Link: https://0day.today/exploit/22561

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: SlowLoris
Type: Trojan
Platform: Script

Malware ID: Redirector
Type: Trojan
Platform: Document,Script

Malware ID: CVE-2014-1510
Type: Exploit
Platform: Script

Malware ID: WebidlInject
Type: Exploit
Platform: Script

Malware ID: CVE-2016-9079
Type: Exploit
Platform: Script

Malware ID: CVE-2014-1511
Type: Exploit
Platform: Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2014-34 through MFSA 2014-47)

| | |
|---|---|
| QID: | 122054 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1518, CVE-2014-1519, CVE-2014-1520, CVE-2014-1522, CVE-2014-1523, CVE-2014-1524, CVE-2014-1525, CVE-2014-1527, CVE-2014-1528, CVE-2014-1529, CVE-2014-1530, CVE-2014-1492, CVE-2014-1532, CVE-2014-1526, CVE-2014-1531 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 66356,67123,67129,67131,67135,67137,67130 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
All Mozilla Firefox versions prior to version 29.0
All Mozilla Firefox ESR version prior to 24.5
All Mozilla Thunderbird version prior to 24.5
All Mozilla SeaMonkey versions prior to 2.26

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=966630

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=944353

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=986678

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=992968

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=980537

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=952022

Reference: CVE-2014-1518
Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=991471

Reference: CVE-2014-1518

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=993546

Reference: CVE-2014-1518

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=986843

Reference: CVE-2014-1519

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=919592

Reference: CVE-2014-1519

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=990794

Reference: CVE-2014-1519

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=953104

Reference: CVE-2014-1520

Description: maintenservice_installer.exe in the Maintenance Service Installer in Mozilla Firefox before 29.0 and Firefox ESR 24.x before 24.5 on Windows allows local users to gain privileges by placing a Trojan horse DLL file into a temporary directory at an unspecified point in the update process.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=961676

Reference: CVE-2014-1522

Description: The mozilla::dom::OscillatorNodeEngine::ComputeCustom function in the Web Audio subsystem in Mozilla Firefox before 29.0 and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read, memory corruption, and application crash) via crafted content.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=995289

Reference: CVE-2014-1524

Description: The nsXBLProtoImpl::InstallImplementation function in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 does not properly check whether objects are XBL objects, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted JavaScript code that accesses a non-XBL object as if it were an XBL object.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=989183

Reference: CVE-2014-1529

Description: The Web Notification API in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to bypass intended source-component restrictions and execute arbitrary JavaScript code in a privileged context via a crafted web page for which Notification.permission is granted.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=987003

Reference: CVE-2014-1531

Description: Use-after-free vulnerability in the nsGenericHTMLElement::GetWidthHeightForImage function in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving an imgLoader object that is not properly handled during an image-resize operation.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=987140

Reference: CVE-2014-1532

Description: Use-after-free vulnerability in the nsHostResolver::ConditionallyRefreshRecord function in libxul.so in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors related to host resolution.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=966006

Reference: CVE-2014-1492

Description: The cert_TestHostName function in lib/certdb/certdb.c in the certificate-checking implementation in Mozilla Network Security Services (NSS) before 3.16 accepts a wildcard character that is embedded in an internationalized domain name's U-label, which might allow man-in-the-middle attackers to spoof SSL servers via a crafted certificate.

Link: https://hg.mozilla.org/projects/nss/rev/709d4e597979

packetstorm
Reference: CVE-2014-1520
Description: Mozilla Firefox DLL Hijacking
Link: https://packetstormsecurity.com/files/137482/Mozilla-Firefox-DLL-Hijacking.html

0day.today
Reference: CVE-2014-1520
Description: Mozilla Arbitrary Code Execution / Privilege Escalation Vulnerability
Link: https://0day.today/exploit/35925

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2014-48 through MFSA 2014-54))

| | |
|---|---|
| QID: | 122131 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1533, CVE-2014-1534, CVE-2014-1536, CVE-2014-1537, CVE-2014-1538, CVE-2014-1540, CVE-2014-1541, CVE-2014-1542, CVE-2014-1543, CVE-2014-1539 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 67965,67964,67966,67971,67976,67978,67979,67968,67969 |
| Service Modified: | 06/02/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. Thunderbird is an email client.
Multiple vulnerabilities have been reported in Mozilla Firefox and Thunderbird:
-Mozilla developers and community identified and fixed several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products.

-Use-after-free and out of bounds read issues are potentially exploitable, allowing for remote code execution.

-A buffer overflow issue exists in the Speex resampler for Web Audio that could lead to code execution.

- A buffer overflow issue exists in the Gamepad API that could lead to code execution.
Affected Software:
All Mozilla Firefox versions prior to version 30.0
All Mozilla Firefox ESR version prior to 24.6
All Mozilla Thunderbird version prior to 24.6

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

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  1.7.0.0

### 4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2014-56 to MFSA 2014-66)

| | |
|---|---|
| QID: | 122469 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1547, CVE-2014-1548, CVE-2014-1549, CVE-2014-1550, CVE-2014-1551, CVE-2014-1561, CVE-2014-1555, CVE-2014-1556, CVE-2014-1544, CVE-2014-1557, CVE-2014-1558, CVE-2014-1559, CVE-2014-1560, CVE-2014-1552 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 68820,68816,68818,68814,68822,68824,68811 |
| Service Modified: | 08/11/2014 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation has released updates to address multiple vulnerabilities for the following.
Affected Versions:
All Mozilla Firefox versions prior to version 31.0.0.0
All Mozilla Firefox ESR version prior to 24.7.0.0
All Mozilla Thunderbird version prior to 31.0.0.0
All Mozilla Thunderbird ESR version prior to 24.7.0.0

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

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  1.7.0.0

### 4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2014-67 to MFSA 2014-72)

| | |
|---|---|
| QID: | 122588 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1562, CVE-2014-1553, CVE-2014-1554, CVE-2014-1563, CVE-2014-1564, CVE-2014-1565, CVE-2014-1566, CVE-2014-1567 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 69524,69526,69519,69523,69525,69521,69522,69520 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |

PCI Vuln: Yes

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
All Mozilla Firefox versions prior to version 32.0.0.0
All Mozilla Firefox ESR version prior to 24.8.0.0
All Mozilla Firefox ESR version prior to 31.1.0.0
All Mozilla Thunderbird version prior to 31.1.0.0
All Mozilla Thunderbird ESR version prior to 24.8.0.0

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Advisory (http://www.mozilla.org/security/announce/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2014-1564
Description: Mozilla Firefox 9.0.1 / Thunderbird 3.1.20 - Information Disclosure - The Exploit-DB Ref : 39295
Link: http://www.exploit-db.com/exploits/39295

exploitdb
Reference: CVE-2014-1564
Description: Mozilla Firefox 9.0.1 / Thunderbird 3.1.20 - Information Disclosure
Link: https://www.exploit-db.com/exploits/39295

packetstorm
Reference: CVE-2014-1564
Description: Mozilla Firefox Secret Leak
Link: https://packetstormsecurity.com/files/128132/Mozilla-Firefox-Secret-Leak.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird/ SeaMonkey NSS Vulnerability (MFSA 2014-73)

| | |
|---|---|
| QID: | 122694 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1568 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 70116 |
| Service Modified: | 10/02/2014 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
The Mozilla Foundation has released updates to address NSS vulnerability.
Affected Versions:
All Mozilla Firefox versions prior to version 32.0.3.0
All Mozilla Firefox ESR version prior to 24.8.1.0
All Mozilla Firefox ESR version prior to 31.1.1.0
All Mozilla Thunderbird version prior to 31.1.2.0
All Mozilla Thunderbird ESR version prior to 24.8.1.0
All Mozilla SeaMonkey versions prior to 2.29.1.

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Advisory (http://www.mozilla.org/security/announce/) , for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Advisory (http://www.mozilla.org/security/announce/)

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  1.7.0.0

## 4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2014-74 to MFSA 2014-82)

| | |
|---|---|
| QID: | 122809 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1583, CVE-2014-1585, CVE-2014-1586, CVE-2014-1582, CVE-2014-1584, CVE-2014-1581, CVE-2014-1580, CVE-2014-1578, CVE-2014-1577, CVE-2014-1576, CVE-2014-1574, CVE-2014-1575 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 70436,70439,70430,70440,70428,70431,70426,70432,70424,70434,70425,70427 |
| Service Modified: | 05/29/2023 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation.

The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 33
Mozilla Firefox ESR versions prior to 31.2
Mozilla Thunderbird versions prior to 31.2

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information and compromise a user's system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:

Following are links for downloading patches to fix the vulnerabilities:
Mozilla Advisory (MFSA 2014-74 to MFSA 2014-82) (https://www.mozilla.org/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2014-1575

Description: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 33.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to improper interaction between threading and garbage collection in the GCRuntime::triggerGC function in js/src/jsgc.cpp, and unknown other vectors.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1023035

packetstorm

Reference: CVE-2014-1580

Description: Firefox / MSIE Memory Disclosure Bugs

Link: https://packetstormsecurity.com/files/128697/Firefox-MSIE-Memory-Disclosure-Bugs.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2014-83 to MFSA 2014-91)

| | |
|---|---|
| QID: | 123014 |
| Category: | Local |
| Associated CVEs: | CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595, CVE-2014-8632, CVE-2014-8631 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 71391,71397,71398,71395,71396 |
| Service Modified: | 12/08/2014 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 34
Mozilla Firefox ESR versions prior to 31.3
Mozilla Thunderbird versions prior to 31.3

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Advisory (MFSA 2014-83 to MFSA 2014-91) (https://www.mozilla.org/security/advisories/)

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  1.7.0.0

### 4 Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2015-01 to MFSA 2015-09)

| | |
|---|---|
| QID: | 123142 |
| Category: | Local |
| Associated CVEs: | CVE-2014-8634, CVE-2014-8635, CVE-2014-8637, CVE-2014-8638, CVE-2014-8639, CVE-2014-8640, CVE-2014-8641, CVE-2014-8643, CVE-2014-8642, CVE-2014-8636 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 72049,72050,72042,72043,72041,72048,72047,72046,72045,72044 |
| Service Modified: | 08/15/2023 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation. SeaMonkey is a suite of applications that includes a browser and an email client.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 35
Mozilla Firefox ESR versions prior to 31.4
Mozilla Thunderbird versions prior to 31.4
Mozilla SeaMonkey versions prior to 2.32

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)
Seamonkey (http://www.seamonkey-project.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit
- Reference: CVE-2014-8636
- Description: Firefox Proxy Prototype Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_proxy_prototype
- Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_proxy_prototype.rb

The Exploit-DB
- Reference: CVE-2014-8636
- Description: Mozilla Firefox - Proxy Prototype Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 36480
- Link: http://www.exploit-db.com/exploits/36480

exploitdb
- Reference: CVE-2014-8636
- Description: Mozilla Firefox - Proxy Prototype Privileged JavaScript Injection (Metasploit)
- Link: https://www.exploit-db.com/exploits/36480

packetstorm

Reference: CVE-2014-8636
Description: Firefox Proxy Prototype Privileged Javascript Injection
Link: https://packetstormsecurity.com/files/130972/Firefox-Proxy-Prototype-Privileged-Javascript-Injection.html

metasploit

Reference: CVE-2014-8636
Description: Firefox Proxy Prototype Privileged Javascript Injection
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2014-8636
Description: Firefox Proxy Prototype Privileged Javascript Injection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_proxy_prototype.rb

0day.today

Reference: CVE-2014-8636
Description: Firefox Proxy Prototype Privileged Javascript Injection Exploit
Link: https://0day.today/exploit/23440

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: Heuristic
Type: Exploit
Platform: Script,Document

Malware ID: FFProxyPrototype
Type: Exploit
Platform: Script

Malware ID: CVE-2014-1511
Type: Exploit
Platform: Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2015-11 to MFSA 2015-27)

| | |
|---|---|
| QID: | 123354 |
| Category: | Local |
| Associated CVEs: | CVE-2015-0836, CVE-2015-0835, CVE-2015-0833, CVE-2015-0832, CVE-2015-0830, CVE-2015-0834, CVE-2015-0831, CVE-2015-0829, CVE-2015-0828, CVE-2015-0827, CVE-2015-0826, CVE-2015-0825, CVE-2015-0824, CVE-2015-0823, CVE-2015-0822, CVE-2015-0821, CVE-2015-0819, CVE-2015-0820 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 72742,72759,72757,72758,72756,72754,72753,72751,72750,72755,72744,72741,72745,72746,72752,72747,72743,72748 |
| Service Modified: | 02/25/2015 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 36

Mozilla Firefox ESR versions prior to 31.5
Mozilla Thunderbird versions prior to 31.5

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

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  1.7.0.0

 4 Mozilla Firefox / SeaMonkey Multiple Vulnerabilities (MFSA 2015-28 through MFSA 2015-29)

| | |
|---|---|
| QID: | 123413 |
| Category: | Local |
| Associated CVEs: | CVE-2015-0818, CVE-2015-0817 |
| Vendor Reference: | Mozilla Advisory |
| Bugtraq ID: | 73265,73263 |
| Service Modified: | 03/31/2015 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Firefox prior to 36.0.4.
Firefox ESR prior to 31.5.3.
SeaMonkey prior to 2.33.1.

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Seamonkey (http://www.seamonkey-project.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)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 4 Mozilla Firefox / Thunderbird Multiple Vulnerabilities (MFSA 2015-30 to MFSA 2015-42)

| | |
|---|---|
| QID: | 123496 |
| Category: | Local |
| Associated CVEs: | CVE-2015-0815, CVE-2015-0814, CVE-2015-0813, CVE-2015-0812, CVE-2015-0816, CVE-2015-0811, CVE-2015-0810, CVE-2015-0808, CVE-2015-0807, CVE-2015-0805, CVE-2015-0806, CVE-2015-0803, CVE-2015-0804, CVE-2015-0801, CVE-2015-0800, CVE-2012-2808, CVE-2015-0802 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-30 to MFSA 2015-42 |
| Bugtraq ID: | 73455,73457,73463,73466,73461 |
| Service Modified: | 08/15/2023 |
| 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. Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 37
Mozilla Firefox ESR versions prior to 31.6
Mozilla Thunderbird versions prior to 31.6

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct man-in-the-middle attacks, gain elevated privileges, disclose sensitive information, bypass same origin policy, compromise a user's system or cause a denial of service condition.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
Mozilla Thunderbird (http://www.mozilla.org/en-US/thunderbird/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2015-0802
Description: Firefox Proxy Prototype Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_proxy_prototype
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_proxy_prototype.rb

Reference: CVE-2015-0816
Description: Firefox PDF.js Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_pdfjs_privilege_escalation
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_pdfjs_privilege_escalation.rb

Reference: CVE-2015-0802
Description: Firefox PDF.js Privileged Javascript Injection - Metasploit Ref : /modules/exploit/multi/browser/firefox_pdfjs_privilege_escalation
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/browser/firefox_pdfjs_privilege_escalation.rb

The Exploit-DB

Reference: CVE-2015-0816
Description: Mozilla Firefox - 'pdf.js' Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 37958
Link: http://www.exploit-db.com/exploits/37958

Reference: CVE-2015-0802
Description: Mozilla Firefox - 'pdf.js' Privileged JavaScript Injection (Metasploit) - The Exploit-DB Ref : 37958
Link: http://www.exploit-db.com/exploits/37958

exploitdb

Reference: CVE-2015-0816
Description: Mozilla Firefox - 'pdf.js' Privileged JavaScript Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/37958

Reference: CVE-2015-0802
Description: Mozilla Firefox - 'pdf.js' Privileged JavaScript Injection (Metasploit)
Link: https://www.exploit-db.com/exploits/37958

nvd

Reference: CVE-2012-2808
Description: The PRNG implementation in the DNS resolver in Bionic in Android before 4.1.1 incorrectly uses time and PID information during the generation of random numbers for query ID values and UDP source ports, which makes it easier for remote attackers to spoof DNS responses by guessing these numbers, a related issue to CVE-2015-0800.
Link: http://blog.watchfire.com/files/androiddnsweakprng.pdf

packetstorm

Reference: CVE-2015-0816
Description: Firefox PDF.js Privileged Javascript Injection
Link: https://packetstormsecurity.com/files/133271/Firefox-PDF.js-Privileged-Javascript-Injection.html

metasploit

Reference: CVE-2015-0816
Description: Firefox PDF.js Privileged Javascript Injection
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2015-0802
Description: Firefox PDF.js Privileged Javascript Injection
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2015-0802
Description: Firefox Proxy Prototype Privileged Javascript Injection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_proxy_prototype.rb

Reference: CVE-2015-0802
Description: Firefox PDF.js Privileged Javascript Injection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_pdfjs_privilege_escalation.rb

Reference: CVE-2015-0816
Description: Firefox PDF.js Privileged Javascript Injection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/browser/firefox_pdfjs_privilege_escalation.rb

0day.today

Reference: CVE-2015-0816
Description: Firefox PDF.js Privileged Javascript Injection Exploit
Link: https://0day.today/exploit/24128

github-exploits

Reference: CVE-2015-0816
Description: Afudadi/Firefox-35-37-Exploit exploit repository

Link: https://github.com/Afudadi/Firefox-35-37-Exploit

Reference: CVE-2015-0802
Description: Afudadi/Firefox-35-37-Exploit exploit repository
Link: https://github.com/Afudadi/Firefox-35-37-Exploit

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: MetaSploit
Type: Hacktool
Platform: Script

Malware ID: RedirME
Type: Trojan
Platform: Document

Malware ID: RemoteShell
Type: Backdoor
Platform: Script

Malware ID: FFPdfjsPrivEsc
Type: Exploit
Platform: Script

Malware ID: CVE-2015-0816
Type: Exploit
Platform: Script

Malware ID: CVE-2015-4495
Type: Exploit
Platform: Script

Malware ID: Heuristic
Type: Exploit
Platform: Script

Malware ID: Evisnefo
Type: Exploit
Platform: Script,Win32

Malware ID: CVE-2010-3187
Type: Exploit
Platform: Unix

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-39 to MFSA 2016-48)

QID: 123719
Category: Local

| | |
|---|---|
| Associated CVEs: | CVE-2016-2820, CVE-2016-2808, CVE-2016-2817, CVE-2016-2816, CVE-2016-2814, CVE-2016-2813, CVE-2016-2811, CVE-2016-2812, CVE-2016-2810, CVE-2016-2809, CVE-2016-2807, CVE-2016-2806, CVE-2016-2804, CVE-2016-2805 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-39 to MFSA 2016-48 |
| Bugtraq ID: | - |
| Service Modified: | 04/28/2016 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 46
Mozilla Firefox ESR versions prior to 38.8
Mozilla Firefox ESR versions prior to 45.1

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can obtain sensitive information, bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-79 to MFSA 2015-92)

| | |
|---|---|
| QID: | 123800 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4477, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4493, CVE-2015-4481, CVE-2015-4482, CVE-2015-4483, CVE-2015-4484, CVE-2015-4491, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4490, CVE-2015-4492 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-79 to MFSA 2015-92 |
| Bugtraq ID: | 76297,76294,76510 |
| Service Modified: | 05/29/2023 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:

Mozilla Firefox versions prior to 40
Mozilla Firefox ESR versions prior to 38.2

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, gain elevated privileges, execute arbitrary code, cause a denial of service condition or conduct cross-site scripting attacks.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2015-4481
Description: Mozilla - Maintenance Service Log File Overwrite Privilege Escalation - The Exploit-DB Ref : 37925
Link: http://www.exploit-db.com/exploits/37925

exploitdb
Reference: CVE-2015-4481
Description: Mozilla - Maintenance Service Log File Overwrite Privilege Escalation
Link: https://www.exploit-db.com/exploits/37925

seebug
Reference: CVE-2015-4481
Description: Mozilla Maintenance Service Log File Overwrite Elevation of Privilege
Link: https://www.seebug.org/vuldb/ssvid-89465

packetstorm
Reference: CVE-2015-4481
Description: Mozilla Maintenance Service Log File Overwrite Elevation Of Privilege
Link: https://packetstormsecurity.com/files/133226/Mozilla-Maintenance-Service-Log-File-Overwrite-Elevation-Of-Privilege.html

0day.today
Reference: CVE-2015-4481
Description: Mozilla Maintenance Service Log File Overwrite Elevation of Privilege Exploit
Link: https://0day.today/exploit/24109

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-94 and MFSA 2015-95)

| | |
|---|---|
| QID: | 123845 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4497, CVE-2015-4498 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-94 to MFSA 2015-95 |
| Bugtraq ID: | 76502,76505 |
| Service Modified: | 12/09/2021 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 40.0.3
Mozilla Firefox ESR versions prior to 38.2.1

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-96 and MFSA 2015-114)

| | |
|---|---|
| QID: | 123970 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4500, CVE-2015-4501, CVE-2015-4503, CVE-2015-4504, CVE-2015-4476, CVE-2015-4505, CVE-2015-4506, CVE-2015-4507, CVE-2015-4508, CVE-2015-4510, CVE-2015-4511, CVE-2015-4509, CVE-2015-4512, CVE-2015-4502, CVE-2015-4516, CVE-2015-4519, CVE-2015-4520, CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180, CVE-2015-7178, CVE-2015-7179 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-96 to MFSA 2015-114 |
| Bugtraq ID: | 76815,76816 |
| Service Modified: | 09/24/2015 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 41
Mozilla Firefox ESR versions prior to 38.3

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, obtain sensitive information, conduct spoofing attacks, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-134 and MFSA 2015-149)

| | |
|---|---|
| QID: | 124406 |
| Category: | Local |
| Associated CVEs: | CVE-2015-7201, CVE-2015-7202, CVE-2015-7204, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7212, CVE-2015-7215, CVE-2015-7211, CVE-2015-7218, CVE-2015-7219, CVE-2015-7216, CVE-2015-7217, CVE-2015-7203, CVE-2015-7220, CVE-2015-7221, CVE-2015-7205, CVE-2015-7213, CVE-2015-7222, CVE-2015-7223, CVE-2015-7214 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-134 to MFSA 2015-149 |
| Bugtraq ID: | 79280,79279,79283,79278 |
| Service Modified: | 12/17/2015 |
| 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.
The Mozilla Foundation
has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 43
Mozilla
Firefox ESR versions prior to 38.5

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can bypass certain security restrictions, obtain sensitive information, conduct spoofing attacks, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-01 to MFSA 2016-12)

| | |
|---|---|
| QID: | 124615 |
| Category: | Local |
| Associated CVEs: | CVE-2016-1930, CVE-2016-1931, CVE-2016-1933, CVE-2016-1935, CVE-2016-1939, CVE-2015-7208, CVE-2016-1940, CVE-2016-1937, CVE-2016-1938, CVE-2016-1941, CVE-2016-1943, CVE-2016-1942, CVE-2016-1944, CVE-2016-1945, CVE-2016-1946, CVE-2016-1947, CVE-2016-1948, CVE-2016-1978 |

| | |
|---|---|
| Vendor Reference: | Mozilla Advisory MFSA 2016-01 to MFSA 2016-12 |
| Bugtraq ID: | 91787,79280,81949,81953,81956,81952,81957,81955,81948,81950 |
| Service Modified: | 05/27/2020 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 44
Mozilla Firefox ESR versions prior to 38.6

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct man-in-the-middle or cookie injection attacks, bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-16 to MFSA 2016-38)

| | |
|---|---|
| QID: | 124781 |
| Category: | Local |
| Associated CVEs: | CVE-2016-1952, CVE-2016-1953, CVE-2016-1954, CVE-2016-1955, CVE-2016-1956, CVE-2016-1957, CVE-2016-1958, CVE-2016-1959, CVE-2016-1960, CVE-2016-1961, CVE-2016-1962, CVE-2016-1963, CVE-2016-1964, CVE-2016-1965, CVE-2016-1967, CVE-2016-1968, CVE-2016-1966, CVE-2016-1970, CVE-2016-1971, CVE-2016-1972, CVE-2016-1975, CVE-2016-1976, CVE-2016-1973, CVE-2016-1974, CVE-2016-1950, CVE-2016-1979, CVE-2016-1977, CVE-2016-2790, CVE-2016-2791, CVE-2016-2792, CVE-2016-2793, CVE-2016-2794, CVE-2016-2795, CVE-2016-2796, CVE-2016-2797, CVE-2016-2798, CVE-2016-2799, CVE-2016-2800, CVE-2016-2801, CVE-2016-2802, CVE-2016-1969 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-16 to MFSA 2016-38 |
| Bugtraq ID: | 84220,84222,84221,84223 |
| Service Modified: | 05/29/2023 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 45
Mozilla Firefox ESR versions prior to 38.7

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can obtain sensitive information, bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2016-1960
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 44294
Link: http://www.exploit-db.com/exploits/44294

Reference: CVE-2016-1960
Description: Mozilla Firefox < 45.0 - 'nsHtml5TreeBuilder' Use-After-Free (EMET 5.52 Bypass) - The Exploit-DB Ref : 42484
Link: http://www.exploit-db.com/exploits/42484

exploitdb

Reference: CVE-2016-1960
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/44294

Reference: CVE-2016-1960
Description: Mozilla Firefox < 45.0 - 'nsHtml5TreeBuilder' Use-After-Free (EMET 5.52 Bypass)
Link: https://www.exploit-db.com/exploits/42484

packetstorm

Reference: CVE-2016-1960
Description: Mozilla Firefox nsHtml5TreeBuilder Use-After-Free
Link: https://packetstormsecurity.com/files/143867/Mozilla-Firefox-nsHtml5TreeBuilder-Use-After-Free.html

Reference: CVE-2016-1960
Description: Firefox 44.0.2 ASM.JS JIT-Spray Remote Code Execution
Link: https://packetstormsecurity.com/files/146819/Firefox-44.0.2-ASM.JS-JIT-Spray-Remote-Code-Execution.html

0day.today

Reference: CVE-2016-1960
Description: Mozilla Firefox < 45.0 - nsHtml5TreeBuilder Use-After-Free (EMET 5.52 Bypass) Exploit
Link: https://0day.today/exploit/28309

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: RemoteShell
Type: Backdoor
Platform: Unix

Malware ID: Heuristic
Type: Trojan
Platform: Script

Malware ID: Cryxos
Type: Trojan
Platform: Script

Malware ID: CVE-2016-1960
Type: Exploit
Platform: Script

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-49 to MFSA 2016-61)

| | |
|---|---|
| QID: | 370056 |
| Category: | Local |
| Associated CVEs: | CVE-2016-2834, CVE-2016-2833, CVE-2016-2832, CVE-2016-2831, CVE-2016-2829, CVE-2016-2828, CVE-2016-2826, CVE-2016-2825, CVE-2016-2824, CVE-2016-2822, CVE-2016-2821, CVE-2016-2819, CVE-2016-2818, CVE-2016-2815 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-49 to MFSA 2016-61 |
| Bugtraq ID: | 91075,91072 |
| Service Modified: | 05/29/2023 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 47
Mozilla Firefox ESR versions prior to 45.2
Mozilla Firefox NSS versions prior to 3.23

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can obtain sensitive information, bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2016-2819
Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution - The Exploit-DB Ref : 44293
Link: http://www.exploit-db.com/exploits/44293

exploitdb
Reference: CVE-2016-2819
Description: Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/44294

Reference: CVE-2016-2819
Description: Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution
Link: https://www.exploit-db.com/exploits/44293

packetstorm
Reference: CVE-2016-2819
Description: Firefox 46.0.1 ASM.JS JIT-Spray Remote Code Execution
Link: https://packetstormsecurity.com/files/146818/Firefox-46.0.1-ASM.JS-JIT-Spray-Remote-Code-Execution.html

ASSOCIATED MALWARE:

ReversingLabs

| | |
|---|---|
| Malware ID: | Heuristic |
| Type: | Trojan |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | Cryxos |
| Type: | Trojan |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | CVE-2016-2819 |
| Type: | Exploit |
| Platform: | Script |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-62 to MFSA 2016-84)

| | |
|---|---|
| QID: | 370108 |
| Category: | Local |
| Associated CVEs: | CVE-2016-2830, CVE-2016-2835, CVE-2016-2836, CVE-2016-2837, CVE-2016-2838, CVE-2016-2839, CVE-2016-5250, CVE-2016-5251, CVE-2016-5252, CVE-2016-5253, CVE-2016-5254, CVE-2016-5255, CVE-2016-5258, CVE-2016-5259, CVE-2016-5260, CVE-2016-5261, CVE-2016-5262, CVE-2016-5263, CVE-2016-5264, CVE-2016-5265, CVE-2016-5266, CVE-2016-5267, CVE-2016-5268 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-62 to MFSA 2016-84 |
| Bugtraq ID: | 92258,92260,92261 |
| Service Modified: | 05/29/2023 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 48
Mozilla Firefox ESR versions prior to 45.3

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can obtain sensitive information, bypass certain security restrictions, execute arbitrary code or cause a denial of service condition on the targeted system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the advisories below:
Mozilla Security Advisories - Main Page (http://www.mozilla.org/security/announce/)
MFSA 2016-62 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-62/)
MFSA 2016-63 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-63/)
MFSA 2016-64 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-64/)
MFSA 2016-65 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-65/)
MFSA 2016-66 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-66/)
MFSA 2016-67 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-67/)
MFSA 2016-68 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-68/)
MFSA 2016-69 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-69/)
MFSA 2016-70 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-70/)
MFSA 2016-71 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-71/)
MFSA 2016-72 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-72/)
MFSA 2016-73 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-73/)
MFSA 2016-74 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-74/)
MFSA 2016-75 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/)

MFSA 2016-76 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-76/)
MFSA 2016-77 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-77/)
MFSA 2016-78 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-78/)
MFSA 2016-79 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-79/)
MFSA 2016-80 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-80/)
MFSA 2016-81 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-81/)
MFSA 2016-82 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-82/)
MFSA 2016-83 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-83/)
MFSA 2016-84 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-84/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)
mfsa2016-62 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-62/ )
mfsa2016-63 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-63/ )
mfsa2016-64 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-64/ )
mfsa2016-65 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-65/ )
mfsa2016-66 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-66/ )
mfsa2016-67 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-67/ )
mfsa2016-68 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-68/ )
mfsa2016-69 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-69/ )
mfsa2016-70 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-70/ )
mfsa2016-71 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-71/ )
mfsa2016-72 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-72/ )
mfsa2016-73 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-73/ )
mfsa2016-74 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-74/ )
mfsa2016-75 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/ )
mfsa2016-76 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-76/ )
mfsa2016-77 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-77/ )
mfsa2016-78 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-78/ )
mfsa2016-79 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-79/ )
mfsa2016-80 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-80/ )
mfsa2016-81 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-81/)
mfsa2016-82 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-82/)
mfsa2016-83 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-83/ )
mfsa2016-84 (https://www.mozilla.org/en-US/security/advisories/mfsa2016-84/ )

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2016-5258
Description: Use-after-free vulnerability in the WebRTC socket thread in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code by leveraging incorrect free operations on DTLS objects during the shutdown of a WebRTC session.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1279146

Reference: CVE-2016-5259
Description: Use-after-free vulnerability in the CanonicalizeXPCOMParticipant function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via a script that closes its own Service Worker within a nested sync event loop.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1282992

Reference: CVE-2016-5264
Description: Use-after-free vulnerability in the nsNodeUtils::NativeAnonymousChildListChange function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an SVG element that is mishandled during effect application.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1286183

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Use After Free Denial of Service Vulnerability

| | |
|---|---|
| QID: | 370392 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5031 |
| Vendor Reference: | mfsa2017-14 |
| Bugtraq ID: | 96767,98326 |

| | |
|---|---|
| Service Modified: | 05/17/2017 |
| 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.
A use-after-free can occur during Buffer11 API calls within the ANGLE graphics library, used for WebGL content. This can lead to a potentially exploitable crash.
Affected Version :
Firefox prior to 53.0.2
Firefox ESR prior to 52.1.1

IMPACT:

An attacker may exploit this issue to crash the affected application, resulting in a denial-of-service condition.

SOLUTION:

The vendor has issued a fix (53.0.2). Refer to MFSA 2017-14 (https://www.mozilla.org/en-US/security/advisories/mfsa2017-14/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2017-14: windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-14/)
mfsa2017-14: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-14/)

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  1.7.0.0

### 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: | 05/30/2023 |
| 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. 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (mfsa2017-27)

| | |
|---|---|
| QID: | 370685 |
| Category: | Local |
| Associated CVEs: | CVE-2017-7843, CVE-2017-7844 |
| Vendor Reference: | mfsa2017-27 |
| Bugtraq ID: | 102039,102112 |
| Service Modified: | 05/30/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox.Visited history information leak through SVG image.
Affected Versions:
Firefox prior to 57.0.1

IMPACT:

A combination of an external SVG image referenced on a page and the coloring of anchor links stored within this image can be used to determine which pages a user has in their history. This can allow a malicious website to query user history.

When Private Browsing mode is used, it is
possible for a web worker to write persistent data to IndexedDB and fingerprint a user uniquely. IndexedDB should not be available in Private Browsing mode and this stored data will persist across multiple private browsing mode sessions because it is not cleared when exiting.

SOLUTION:

The vendor has issued a fix (57.0.1).
Refer to MFSA 2017-27 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2017-27: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2017-27/)
MFSA 2017-27: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2017-27/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2017-7843
Description: When Private Browsing mode is used, it is possible for a web worker to write persistent data to IndexedDB and fingerprint a user uniquely. IndexedDB should not be available in Private Browsing mode and this stored data will persist across multiple private browsing mode sessions because it is not cleared when exiting. This vulnerability affects Firefox ESR < 52.5.2 and Firefox < 57.0.1.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1410106

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Spectre Vulnerability (MFSA2018-01)(Spectre)

| | |
|---|---|
| QID: | 370712 |
| Category: | Local |
| Associated CVEs: | CVE-2017-5753, CVE-2017-5715 |
| Vendor Reference: | MFSA2018-01 |
| Bugtraq ID: | 102371,102376 |
| Service Modified: | 08/17/2023 |
| 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.
Speculative execution side-channel attack ("Spectre") was reported in Mozilla Firefox.
Affected Version:
Firefox prior to 57.0.4

IMPACT:

N/A

SOLUTION:

The vendor has issued a fix (57.0.4).
Refer to MFSA 2018-01 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2018-01: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)
MFSA 2018-01: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2017-5753
Description: Multiple CPUs - 'Spectre' Information Disclosure - The Exploit-DB Ref : 43427
Link: http://www.exploit-db.com/exploits/43427

Reference: CVE-2017-5715
Description: Multiple CPUs - 'Spectre' Information Disclosure - The Exploit-DB Ref : 43427
Link: http://www.exploit-db.com/exploits/43427

exploitdb
Reference: CVE-2017-5715
Description: Multiple CPUs - 'Spectre' Information Disclosure
Link: https://www.exploit-db.com/exploits/43427

Reference: CVE-2017-5753
Description: Multiple CPUs - 'Spectre' Information Disclosure
Link: https://www.exploit-db.com/exploits/43427

nvd
Reference: CVE-2017-5715
Description: Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
Link: https://www.exploit-db.com/exploits/43427/

Reference: CVE-2017-5715
Description: Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
Link: http://packetstormsecurity.com/files/145645/Spectre-Information-Disclosure-Proof-Of-Concept.html

Reference: CVE-2017-5753
Description: Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
Link: https://www.exploit-db.com/exploits/43427/

Reference: CVE-2017-5753
Description: Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
Link: http://packetstormsecurity.com/files/145645/Spectre-Information-Disclosure-Proof-Of-Concept.html

seebug
Reference: CVE-2017-5715
Description: Reading privileged memory with a side-channel (Meltdown & Spectre)
Link: https://www.seebug.org/vuldb/ssvid-97059

Reference: CVE-2017-5753
Description: Reading privileged memory with a side-channel (Meltdown & Spectre)
Link: https://www.seebug.org/vuldb/ssvid-97059

packetstorm
Reference: CVE-2017-5715
Description: Spectre Information Disclosure Proof Of Concept
Link: https://packetstormsecurity.com/files/145645/Spectre-Information-Disclosure-Proof-Of-Concept.html

Reference: CVE-2017-5753
Description: Spectre Information Disclosure Proof Of Concept
Link: https://packetstormsecurity.com/files/145645/Spectre-Information-Disclosure-Proof-Of-Concept.html

0day.today
Reference: CVE-2017-5715
Description: Multiple CPUs - Spectre Information Disclosure (PoC) Exploit
Link: https://0day.today/exploit/29366

Reference: CVE-2017-5753
Description: Multiple CPUs - Spectre Information Disclosure (PoC) Exploit
Link: https://0day.today/exploit/29366

github-exploits

Reference: CVE-2017-5753
Description: Eugnis/spectre-attack exploit repository
Link: https://github.com/Eugnis/spectre-attack

Reference: CVE-2017-5715
Description: opsxcq/exploit-cve-2017-5715 exploit repository
Link: https://github.com/opsxcq/exploit-cve-2017-5715

Reference: CVE-2017-5753
Description: pedrolucasoliva/spectre-attack-demo exploit repository
Link: https://github.com/pedrolucasoliva/spectre-attack-demo

Reference: CVE-2017-5753
Description: albertleecn/cve-2017-5753 exploit repository
Link: https://github.com/albertleecn/cve-2017-5753

Reference: CVE-2017-5753
Description: EdwardOwusuAdjei/Spectre-PoC exploit repository
Link: https://github.com/EdwardOwusuAdjei/Spectre-PoC

Reference: CVE-2017-5753
Description: poilynx/spectre-attack-example exploit repository
Link: https://github.com/poilynx/spectre-attack-example

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: Generic
Type: Trojan
Platform: Win32,Binary

Malware ID: Spectre
Type: Trojan
Platform: Script

Malware ID: Mirai
Type: Trojan
Platform: Linux

Malware ID: Ursu
Type: Trojan
Platform: Win32

Malware ID: Tiggre
Type: Trojan
Platform: Win32

Malware ID: Zusy
Type: Trojan
Platform: Win32

Malware ID: Miner
Type: Trojan
Platform: Win32

| | |
|---|---|
| Malware ID: | Zpevdo |
| Type: | Trojan |
| Platform: | Win32 |

| | |
|---|---|
| Malware ID: | Wacatac |
| Type: | Trojan |
| Platform: | Win32 |

| | |
|---|---|
| Malware ID: | Occamy |
| Type: | Trojan |
| Platform: | Win32 |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-03 , MFSA2018-02)

| | |
|---|---|
| QID: | 370739 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5091, CVE-2018-5092, CVE-2018-5093, CVE-2018-5094, CVE-2018-5095, CVE-2018-5097, CVE-2018-5098, CVE-2018-5099, CVE-2018-5100, CVE-2018-5101, CVE-2018-5102, CVE-2018-5103, CVE-2018-5104, CVE-2018-5105, CVE-2018-5106, CVE-2018-5107, CVE-2018-5108, CVE-2018-5109, CVE-2018-5110, CVE-2018-5111, CVE-2018-5112, CVE-2018-5113, CVE-2018-5114, CVE-2018-5115, CVE-2018-5116, CVE-2018-5117, CVE-2018-5118, CVE-2018-5119, CVE-2018-5121, CVE-2018-5122, CVE-2018-5090, CVE-2018-5089, CVE-2018-5096 |
| Vendor Reference: | MFSA2018-02, MFSA2018-03 |
| Bugtraq ID: | 102783,102786,102771 |
| Service Modified: | 06/18/2020 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox:
CVE-2018-5091: Use-after-free with DTMF timers
CVE-2018-5092: Use-after-free in Web Workers
CVE-2018-5093: Buffer overflow in WebAssembly during Memory/Table resizing
CVE-2018-5094: Buffer overflow in WebAssembly with garbage collection on uninitialized memory
CVE-2018-5095: Integer overflow in Skia library during edge builder allocation
CVE-2018-5097: Use-after-free when source document is manipulated during XSLT
CVE-2018-5098: Use-after-free while manipulating form input elements
CVE-2018-5099: Use-after-free with widget listener
CVE-2018-5100: Use-after-free when IsPotentiallyScrollable arguments are freed from memory
CVE-2018-5101: Use-after-free with floating first-letter style elements
CVE-2018-5102: Use-after-free in HTML media elements
CVE-2018-5103: Use-after-free during mouse event handling
CVE-2018-5104: Use-after-free during font face manipulation
CVE-2018-5105: WebExtensions can save and execute files on local file system without user prompts
CVE-2018-5106: Developer Tools can expose style editor information cross-origin through service worker
CVE-2018-5107: Printing process will follow symlinks for local file access
CVE-2018-5108: Manually entered blob URL can be accessed by subsequent private browsing tabs
CVE-2018-5109: Audio capture prompts and starts with incorrect origin attribution
CVE-2018-5110: Cursor can be made invisible on OS X
CVE-2018-5111: URL spoofing in addressbar through drag and drop
CVE-2018-5112: Extension development tools panel can open a non-relative URL in the panel
CVE-2018-5113: WebExtensions can load non-HTTPS pages with browser.identity.launchWebAuthFlow
CVE-2018-5114: The old value of a cookie changed to HttpOnly remains accessible to scripts
CVE-2018-5115: Background network requests can open HTTP authentication in unrelated foreground tabs
CVE-2018-5116: WebExtension ActiveTab permission allows cross-origin frame content access
CVE-2018-5117: URL spoofing with right-to-left text aligned left-to-right
CVE-2018-5118: Activity Stream images can attempt to load local content through file:
CVE-2018-5119: Reader view will load cross-origin content in violation of CORS headers
CVE-2018-5121: OS X Tibetan characters render incompletely in the addressbar

CVE-2018-5122: Potential integer overflow in DoCrypt
CVE-2018-5090: Memory safety bugs
CVE-2018-5089: Memory safety bugs
CVE-2018-5096: Use-after-free while editing form elements
Affected Versions:
Firefox prior to 58
Firefox ESR prior to 52.6

IMPACT:

A remote user can cause arbitrary code to be executed on the target user's system. A remote user can bypass security controls on the target system. A remote user can spoof URLs.

SOLUTION:

Refer to mfsa2018-03 and mfsa2018-02 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-03 and mfsa2018-02: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
mfsa2018-03 and mfsa2018-02: Windows (https://www.mozilla.org/en-US/security/advisories/)

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 1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-06 , MFSA2018-07)

| | |
|---|---|
| QID: | 370821 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5127, CVE-2018-5128, CVE-2018-5129, CVE-2018-5130, CVE-2018-5131, CVE-2018-5132, CVE-2018-5133, CVE-2018-5134, CVE-2018-5135, CVE-2018-5136, CVE-2018-5137, CVE-2018-5138, CVE-2018-5140, CVE-2018-5141, CVE-2018-5142, CVE-2018-5143, CVE-2018-5126, CVE-2018-5125, CVE-2018-5144, CVE-2018-5145 |
| Vendor Reference: | MFSA2018-06, MFSA2018-07 |
| Bugtraq ID: | 103386,103384,103388 |
| Service Modified: | 06/18/2020 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox:
CVE-2018-5126: Memory safety bugs fixed in Firefox 59
CVE-2018-5125: Memory safety bugs fixed in Firefox 59 and Firefox ESR 52.7
CVE-2018-5127: Buffer overflow manipulating SVG animatedPathSegList
CVE-2018-5128: Use-after-free manipulating editor selection ranges
CVE-2018-5129: Out-of-bounds write with malformed IPC messages
CVE-2018-5130: Mismatched RTP payload type can trigger memory corruption
CVE-2018-5131: Fetch API improperly returns cached copies of no-store/no-cache resources
CVE-2018-5132: WebExtension Find API can search privileged pages
CVE-2018-5133: Value of the app.support.baseURL preference is not properly sanitized
CVE-2018-5134: WebExtensions may use view-source: URLs to bypass content restrictions
CVE-2018-5135: WebExtension browserAction can inject scripts into unintended contexts
CVE-2018-5136: Same-origin policy violation with data: URL shared workers
CVE-2018-5137: Script content can access legacy extension non-contentaccessible resources
CVE-2018-5138: Android Custom Tab address spoofing through long domain names
CVE-2018-5140: Moz-icon images accessible to web content through moz-icon: protocol
CVE-2018-5141: DOS attack through notifications Push API

CVE-2018-5142: Media Capture and Streams API permissions display incorrect origin with data: and blob: URLs
CVE-2018-5143: Self-XSS pasting javascript: URL with embedded tab into addressbar
CVE-2018-5144: Integer overflow during Unicode conversion
CVE-2018-5145: Memory safety bugs fixed in Firefox ESR 52.7
Affected Versions:
Firefox prior to 59
Firefox ESR prior to 52.7

IMPACT:

A remote user can cause arbitrary code to be executed on the target user's system. A remote user can bypass security controls on the target system. A remote user can spoof URLs.

SOLUTION:

Refer to mfsa2018-07 and  mfsa2018-06 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-07 and  mfsa2018-06: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
mfsa2018-07 and  mfsa2018-06: Windows (https://www.mozilla.org/en-US/security/advisories/)

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  1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-08)

| | |
|---|---|
| QID: | 370827 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5146, CVE-2018-5147 |
| Vendor Reference: | MFSA2018-08 |
| Bugtraq ID: | 103432 |
| Service Modified: | 06/18/2020 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox:
CVE-2018-5146: Out of bounds memory write in libvorbis
CVE-2018-5147: Out of bounds memory write in libtremor
Affected Versions:
Firefox prior to 59.0.1
Firefox ESR prior to 52.7.2

IMPACT:

Successful exploitation allows attacker to gain access to sensitive information.

SOLUTION:

Refer to mfsa2018-08 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-08: Windows (https://www.mozilla.org/en-US/security/advisories/)
mfsa2018-08: MAC (https://www.mozilla.org/en-US/security/advisories/)

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  1.7.0.0

### 4 Mozilla Firefox Use-after-free in compositor Vulnerability (MFSA2018-10)

| | |
|---|---|
| QID: | 370836 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5148 |
| Vendor Reference: | MFSA2018-10 |
| Bugtraq ID: | 103506 |
| Service Modified: | 06/18/2020 |
| 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.
CVE-2018-5148: Use-after-free in compositor
Affected Versions:
Firefox prior to 59.0.2
Firefox ESR prior to 52.7.3

IMPACT:

Successful exploitation of this vulnerability could result in a potentially exploitable crash.

SOLUTION:

Refer to MFSA2018-10 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/)
mfsa2018-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/)

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  1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-11 and MFSA2018-12)

| | |
|---|---|
| QID: | 370938 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5183, CVE-2018-5178, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5160, CVE-2018-5152, CVE-2018-5153, CVE-2018-5163, CVE-2018-5164, CVE-2018-5166, CVE-2018-5167, CVE-2018-5168, CVE-2018-5169, CVE-2018-5172, CVE-2018-5173, CVE-2018-5174, CVE-2018-5175, CVE-2018-5176, CVE-2018-5177, CVE-2018-5165, CVE-2018-5180, CVE-2018-5181, CVE-2018-5182, CVE-2018-5151, CVE-2018-5150 |

| | |
|---|---|
| Vendor Reference: | MFSA2018-11, MFSA2018-12 |
| Bugtraq ID: | 104139,104136,104138 |
| Service Modified: | 05/30/2023 |
| 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.
Multiple vulnerabilities were reported in Mozilla Firefox:
CVE-2018-5183: Backport critical security fixes in Skia
CVE-2018-5178: Buffer overflow during UTF-8 to Unicode string conversion through legacy extension
CVE-2018-5154: Use-after-free with SVG animations and clip paths
CVE-2018-5155: Use-after-free with SVG animations and text paths
CVE-2018-5157: Same-origin bypass of PDF Viewer to view protected PDF files

CVE-2018-5158: Malicious PDF can inject JavaScript into PDF Viewer

CVE-2018-5159: Integer overflow and out-of-bounds write in Skia

CVE-2018-5160: Uninitialized memory use by WebRTC encoder

CVE-2018-5152: WebExtensions information leak through webRequest API

CVE-2018-5153: Out-of-bounds read in mixed content websocket messages

CVE-2018-5163: Replacing cached data in JavaScript Start-up Bytecode Cache

CVE-2018-5164: CSP not applied to all multipart content sent with multipart/x-mixed-replace

CVE-2018-5166: WebExtension host permission bypass through filterReponseData

CVE-2018-5167: Improper linkification of chrome: and javascript: content in web console and JavaScript debugger

CVE-2018-5168: Lightweight themes can be installed without user interaction

CVE-2018-5169: Dragging and dropping link text onto home button can set home page to include chrome pages

CVE-2018-5172: Pasted script from clipboard can run in the Live Bookmarks page or PDF viewer

CVE-2018-5173: File name spoofing of Downloads panel with Unicode characters

CVE-2018-5174: Windows Defender SmartScreen UI runs with less secure behavior for downloaded files in Windows 10 April 2018 Update

CVE-2018-5175: Universal CSP bypass on sites using strict-dynamic in their policies

CVE-2018-5176: JSON Viewer script injection

CVE-2018-5177: Buffer overflow in XSLT during number formatting

CVE-2018-5165: Checkbox for enabling Flash protected mode is inverted in 32-bit Firefox

CVE-2018-5180: heap-use-after-free in mozilla::WebGLContext::DrawElementsInstanced

CVE-2018-5181: Local file can be displayed in noopener tab through drag and drop of hyperlink

CVE-2018-5182: Local file can be displayed from hyperlink dragged and dropped on addressbar

CVE-2018-5151: Memory safety bugs fixed in Firefox 60
CVE-2018-5150: Memory safety bugs fixed in Firefox 60 and Firefox ESR 52.8
Affected Versions:
Firefox prior to 60
Firefox ESR prior to 52.8

IMPACT:

If these vulnerabilities are successfully exploited, an attacker can conduct spoofing attacks, bypass certain security restrictions, disclose sensitive information, compromise a user's system or cause a denial of service condition.

SOLUTION:

Refer to mfsa2018-11 and mfsa2018-12 (https://www.mozilla.org/en-US/security/advisories/) .
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-11: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
mfsa2018-11: Windows (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2018-5159
Description: Skia and Firefox - Integer Overflow in SkTDArray Leading to Out-of-Bounds Write - The Exploit-DB Ref : 44759
Link: http://www.exploit-db.com/exploits/44759

exploitdb

Reference: CVE-2018-5159
Description: Skia and Firefox - Integer Overflow in SkTDArray Leading to Out-of-Bounds Write
Link: https://www.exploit-db.com/exploits/44759

nvd

Reference: CVE-2018-5159
Description: An integer overflow can occur in the Skia library due to 32-bit integer use in an array without integer overflow checks, resulting in possible out-of-bounds writes. This could lead to a potentially exploitable crash triggerable by web content. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
Link: https://www.exploit-db.com/exploits/44759/

Reference: CVE-2018-5165
Description: In 32-bit versions of Firefox, the Adobe Flash plugin setting for "Enable Adobe Flash protected mode" is unchecked by default even though the Adobe Flash sandbox is actually enabled. The displayed state is the reverse of the true setting, resulting in user confusion. This could cause users to select this setting intending to activate it and inadvertently turn protections off. This vulnerability affects Firefox < 60.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1451452

Reference: CVE-2018-5181
Description: If a URL using the "file:" protocol is dragged and dropped onto an open tab that is running in a different child process the tab will open a local file corresponding to the dropped URL, contrary to policy. One way to make the target tab open more reliably in a separate process is to open it with the "noopener" keyword. This vulnerability affects Firefox < 60.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1424107

packetstorm

Reference: CVE-2018-5159
Description: Skia / Firefox SkTDArray Integer Overflow
Link: https://packetstormsecurity.com/files/147843/Skia-Firefox-SkTDArray-Integer-Overflow.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA-2018-24)

| | |
|---|---|
| QID: | 371231 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12386, CVE-2018-12387 |
| Vendor Reference: | MFSA2018-24 |
| Bugtraq ID: | 105460 |
| Service Modified: | 07/31/2023 |
| 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.Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox ESR, which could allow for arbitrary code execution.
CVE-2018-12386: register allocation in JavaScript can lead to type confusion.
CVE-2018-12387:JavaScript JIT compiler inlines Array.prototype.push with multiple arguments.

Affected Products:
Prior to Firefox 62.0.3
Prior to Firefox ESR 60.2.2

IMPACT:

On successful exploitation it could allow a remote attacker to execute code.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2018-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-24)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2018-24: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-24)
MFSA2018-24: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-24)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2018-12386
Description: A vulnerability in register allocation in JavaScript can lead to type confusion, allowing for an arbitrary read and write. This leads to remote code execution inside the sandboxed content process when triggered. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1493900

Reference: CVE-2018-12387
Description: A vulnerability where the JavaScript JIT compiler inlines Array.prototype.push with multiple arguments that results in the stack pointer being off by 8 bytes after a bailout. This leaks a memory address to the calling function which can be used as part of an exploit inside the sandboxed content process. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1493903

github-exploits

Reference: CVE-2018-12386
Description: 0xLyte/cve-2018-12386 exploit repository
Link: https://github.com/0xLyte/cve-2018-12386

Reference: CVE-2018-12386
Description: Hydra3evil/cve-2018-12386 exploit repository
Link: https://github.com/Hydra3evil/cve-2018-12386

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA-2018-26 MFSA-2018-27 )

| | |
|---|---|
| QID: | 371276 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12388, CVE-2018-12389, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12398, CVE-2018-12399, CVE-2018-123400, CVE-2018-12401, CVE-2018-12402, CVE-2018-12403, CVE-2018-12400 |
| Vendor Reference: | MFSA2018-26, MFSA2018-27 |
| Bugtraq ID: | 105718,105721,105723,105769 |
| Service Modified: | 06/18/2020 |
| 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.Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox ESR, which could allow for arbitrary code execution.
CVE-2018-12388: Memory safety bugs fixed in Firefox 63
CVE-2018-12389: Memory safety bugs fixed in Firefox ESR 60.3
CVE-2018-12390: Memory safety bugs fixed in Firefox 63 and Firefox ESR 60.3
CVE-2018-12391: HTTP Live Stream audio data is accessible cross-origin
CVE-2018-12392: Crash with nested event loops
CVE-2018-12393: Integer overflow during Unicode conversion while loading JavaScript
CVE-2018-12395: WebExtension bypass of domain restrictions through header rewriting
CVE-2018-12396: WebExtension content scripts can execute in disallowed contexts
CVE-2018-12397: WebExtension bugs
CVE-2018-12398: CSP bypass through stylesheet injection in resource URIs
CVE-2018-12399: Spoofing of protocol registration notification bar
CVE-2018-12400: Favicons are cached in private browsing mode on Firefox for Android
CVE-2018-12401: DOS attack through special resource URI parsing
CVE-2018-12402: SameSite cookies leak when pages are explicitly saved
CVE-2018-12403: Mixed content warning is not displayed when HTTPS page loads a favicon over HTTP
Affected Products:
Prior to Firefox 63.0.0
Prior to Firefox ESR 60.3.0

IMPACT:

On successful exploitation it could allow a remote attacker to execute code.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2018-26 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-26) And MFSA2018-27 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-27)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2018-26 MFSA2018-27: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)
MFSA2018-26 MFSA2018-27: Windows (https://www.mozilla.org/en-US/security/advisories/)

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  1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2018-29 MFSA 2018-30)

| | |
|---|---|
| QID: | 371374 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12407, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18495, CVE-2018-18496, CVE-2018-18497, CVE-2018-18498, CVE-2018-12406, CVE-2018-12405 |
| Vendor Reference: | MFSA 2018-29, MFSA 2018-30 |
| Bugtraq ID: | 105666,106168,106167 |
| Service Modified: | 05/30/2023 |
| 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
Vulnerabilities have been discovered in Mozilla Firefox and Firefox ESR, which could allow for arbitrary code execution

CVE-2018-12407: Buffer overflow with ANGLE library when using VertexBuffer11 module fixed in firefox 64
CVE-2018-17466: Buffer overflow and out-of-bounds read in ANGLE library with TextureStorage11 fixed in Firefox 64
CVE-2018-18492: Use-after-free with select element fixed in Firefox 64

CVE-2018-18493: Buffer overflow in accelerated 2D canvas with Skia fixed in Firefox 64
CVE-2018-18494: Same-origin policy violation using location attribute and performance.getEntries to steal cross-origin URLs fixed in Firefox 64
CVE-2018-18495: WebExtension content scripts can be loaded in about: pages fixed in Firefox 64
CVE-2018-18496: Embedded feed preview page can be abused for clickjacking fixed in Firefox 64
CVE-2018-18497: WebExtensions can load arbitrary URLs through pipe separators fixed in Firefox 64
CVE-2018-18498: Integer overflow when calculating buffer sizes for images fixed in Firefox 64
CVE-2018-12406: Memory safety bugs fixed in Firefox 64
CVE-2018-12405: Memory safety bugs fixed in Firefox 64 and Firefox ESR 60.4
CVE-2018-17466: Buffer overflow and out-of-bounds read in ANGLE library with TextureStorage11 fixed in Firefox ESR 60.4
Affected Products:
Prior to Firefox 64
Prior to Firefox ESR 60.4

IMPACT:

On successful exploitation it could allow a remote attacker to execute code.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2018-29 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-29) And MFSA2018-30 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-30)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2018-29 MFSA 2018-30: Windows (https://www.mozilla.org/en-US/security/advisories)
MFSA 2018-29 MFSA 2018-30: MAC OS X (https://www.mozilla.org/en-US/security/advisories)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2018-12406
Description: Mozilla developers and community members reported memory safety bugs present in Firefox 63. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 64.
Link: https://www.mozilla.org/security/advisories/mfsa2018-29/

Reference: CVE-2018-12406
Description: Mozilla developers and community members reported memory safety bugs present in Firefox 63. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 64.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1456947%2C1475669%2C1504816%2C1502886%2C1500064%2C1500310%2C1500696%2C1499198%

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2019-01 MFSA 2019-02 )

| | |
|---|---|
| QID: | 371615 |
| Category: | Local |
| Associated CVEs: | CVE-2018-18500, CVE-2018-18501, CVE-2018-18502, CVE-2018-18503, CVE-2018-18504, CVE-2018-18505, CVE-2018-18506 |
| Vendor Reference: | MFSA 2019-01, MFSA 2019-02 |
| Bugtraq ID: | 106781,106773 |
| Service Modified: | 07/08/2022 |
| 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
Vulnerabilities have been discovered in Mozilla Firefox and Firefox ESR, which could allow for arbitrary code execution

CVE-2018-18500:Use-after-free parsing HTML5 stream
CVE-2018-18501: Memory safety bugs fixed in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5
CVE-2018-18503: Memory corruption with Audio Buffer
CVE-2018-18504: Memory corruption and out-of-bounds read of texture client buffer
CVE-2018-18505: Privilege escalation through IPC channel messages
CVE-2018-18506: Proxy Auto-Configuration file can define localhost access to be proxied
CVE-2018-18502: Memory safety bugs fixed in Firefox 65
Affected Products:
Prior to Firefox 65
Prior to Firefox ESR 60.5

IMPACT:

On successful exploitation it could allow a remote attacker to execute code.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2019-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-01/) And MFSA2019-02 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-02/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2019-01: Windows (https://www.mozilla.org/en-US/security/advisories/)
mfsa2019-02: MAC OS X (https://www.mozilla.org/en-US/security/advisories/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

ReversingLabs

| | |
|---|---|
| Malware ID: | CVE-2018-18500 |
| Type: | Exploit |
| Platform: | Script |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities(MFSA 2019-04,MFSA2019-05)

| | |
|---|---|
| QID: | 371649 |
| Category: | Local |
| Associated CVEs: | CVE-2018-18356, CVE-2019-5785, CVE-2018-18335 |
| Vendor Reference: | MFSA 2019-04, MFSA2019-05 |
| Bugtraq ID: | 106084 |
| Service Modified: | 05/30/2023 |
| 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
Vulnerabilities discovered in Mozilla Firefox and Firefox ESR:
CVE-2018-18356: A use-after-free vulnerability in the Skia library can occur when creating a path, leading to a potentially exploitable crash.
CVE-2019-5785: An integer overflow vulnerability in the Skia library can occur after specific transform operations, leading to a potentially exploitable crash.
CVE-2018-18335: A buffer overflow vulnerability in the Skia library can occur with Canvas 2D acceleration on macOS. This issue was addressed by disabling Canvas 2D acceleration in Firefox ESR.
Affected Versions:
Prior to Firefox 65.0.1
Prior to Firefox ESR 60.5.1

IMPACT:

On successful exploitation, it could lead to a potentially exploitable crash.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2019-04 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-04/)
And MFSA2019-05 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-04: Windows, Mac (https://www.mozilla.org/en-US/security/advisories/mfsa2019-04/)
MFSA2019-05: Windows, Mac (https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2018-18356
Description: An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
Link: https://crbug.com/883666

Reference: CVE-2019-5785
Description: Incorrect convexity calculations in Skia in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
Link: https://crbug.com/899689

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox and Firefox ESR Arbitrary Code Execution Vulnerability (MFSA2019-19)

| | |
|---|---|
| QID: | 371851 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11708 |
| Vendor Reference: | MFSA2019-19 |
| Bugtraq ID: | - |
| Service Modified: | 10/12/2023 |
| 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.
CVE-2019-11708: Sandbox escape using Prompt:Open
Affected Products: Prior to Firefox 67.0.4 and Firefox ESR 60.7.2

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/#CVE-2019-11708)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/#CVE-2019-11708)
MFSA2019-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-19/#CVE-2019-11708)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2019-11708
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack - The Exploit-DB Ref : 47752
Link: http://www.exploit-db.com/exploits/47752

exploitdb

Reference: CVE-2019-11708
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack
Link: https://www.exploit-db.com/exploits/47752

packetstorm

Reference: CVE-2019-11708
Description: Mozilla Firefox Windows 64-Bit Chain Exploit
Link: https://packetstormsecurity.com/files/155592/Mozilla-Firefox-Windows-64-Bit-Chain-Exploit.html

Reference: CVE-2019-11708
Description: Mozilla Firefox 67 Array.pop JIT Type Confusion
Link: https://packetstormsecurity.com/files/165816/Mozilla-Firefox-67-Array.pop-JIT-Type-Confusion.html

0day.today

Reference: CVE-2019-11708
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack Exploit
Link: https://0day.today/exploit/33639

github-exploits

Reference: CVE-2019-11708
Description: 0vercl0k/CVE-2019-11708 exploit repository
Link: https://github.com/0vercl0k/CVE-2019-11708

cisa-kev

Reference: CVE-2019-11708
Description: Mozilla Firefox and Thunderbird Sandbox Escape Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

gitee-exploits

Reference: CVE-2019-11708
Description: mirrors_0vercl0k/CVE-2019-11708 exploit repository
Link: https://gitee.com/mirrors_0vercl0k/CVE-2019-11708

google-0day-itw

Reference: CVE-2019-11708
Description: Mozilla Firefox Sandbox escape in Prompt:Open
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

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: | 05/30/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 4 Mozilla Firefox and Firefox ESR Multiple Vulnerabilities (MFSA2019-33)(MFSA2019-34)

| | |
|---|---|
| QID: | 372176 |
| Category: | Local |
| Associated CVEs: | CVE-2018-6156, CVE-2019-15903, CVE-2019-11757, CVE-2019-11759, CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763, CVE-2019-11765, CVE-2019-17000, CVE-2019-17001, CVE-2019-17002, CVE-2019-11764, CVE-2019-11758, CVE-2020-12412 |
| Vendor Reference: | MFSA2019-33, MFSA2019-34 |
| Bugtraq ID: | - |
| Service Modified: | 05/30/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefoxis a free and open source web browser which is made by the Mozilla Foundation and its subsidiary, the Mozilla Corporation. It works on common operating systems, such as Windows, macOS, Linux and Android.

Affected Products:
Prior to Firefox 70 and Firefox ESR 68.2

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-34 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-34)
Refer to MFSA2019-33 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-33)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-34: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-34)
MFSA2019-34: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-34)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-15903
Description: In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read.
Link: https://github.com/libexpat/libexpat/issues/317

Reference: CVE-2019-11758
Description: Mozilla community member Philipp reported a memory safety bug present in Firefox 68 when 360 Total Security was installed. This bug showed evidence of memory corruption in the accessibility engine and we presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Firefox < 69, Thunderbird < 68.2, and Firefox ESR < 68.2.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1536227

Reference: CVE-2019-11764
Description: Mozilla developers and community members reported memory safety bugs present in Firefox 69 and Firefox ESR 68.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
Link:
https://bugzilla.mozilla.org/buglist.cgi?bug_id=1558522%2C1577061%2C1548044%2C1571223%2C1573048%2C1578933%2C1575217%2C1583684%

Reference: CVE-2019-17002
Description: If upgrade-insecure-requests was specified in the Content Security Policy, and a link was dragged and dropped from that page, the link was not upgraded to https. This vulnerability affects Firefox < 70.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1561056

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox and ESR Multiple Vulnerabilities (MFSA 2019-07)(MFSA 2019-08)

| | |
|---|---|
| QID: | 372190 |
| Category: | Local |
| Associated CVEs: | CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9797, CVE-2019-9798, CVE-2019-9799, CVE-2019-9801, CVE-2019-9802, CVE-2019-9803, CVE-2019-9804, CVE-2019-9805, CVE-2019-9806, CVE-2019-9807, CVE-2019-9809, CVE-2019-9808, CVE-2019-9789, CVE-2019-9788, CVE-2018-18506 |
| Vendor Reference: | MFSA 2019-07, MFSA 2019-08 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2019-9790: Use-after-free when removing in-use DOM elements

CVE-2019-9791: Type inference is incorrect for constructors entered through on-stack replacement with IonMonkey

CVE-2019-9792: IonMonkey leaks JS_OPTIMIZED_OUT magic value to script

CVE-2019-9793: Improper bounds checks when Spectre mitigations are disabled

CVE-2019-9794: Command line arguments not discarded during execution

CVE-2019-9795: Type-confusion in IonMonkey JIT compiler

CVE-2019-9796: Use-after-free with SMIL animation controller

CVE-2019-9797: Cross-origin theft of images with createImageBitmap

CVE-2019-9798: Library is loaded from world writable APITRACE_LIB location

CVE-2019-9799: Information disclosure via IPC channel messages

CVE-2019-9801: Windows programs that are not 'URL Handlers' are exposed to web content

CVE-2019-9802: Chrome process information leak

CVE-2019-9803: Upgrade-Insecure-Requests incorrectly enforced for same-origin navigation

CVE-2019-9804: Code execution through 'Copy as cURL' in Firefox Developer Tools on macOS

CVE-2019-9805: Potential use of uninitialized memory in Prio

CVE-2019-9806: Denial of service through successive FTP authorization prompts

CVE-2019-9807: Text sent through FTP connection can be incorporated into alert messages

CVE-2019-9809: Denial of service through FTP modal alert error messages

CVE-2019-9808: WebRTC permissions can display incorrect origin with data: and blob: URLs

CVE-2019-9789: Memory safety bugs fixed in Firefox 66

CVE-2019-9788: Memory safety bugs fixed in Firefox 66 and Firefox ESR 60.6
Affected Products : Prior to Firefox 66 and Firefox ESR 60.6

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2019-07 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-07)
Vendor has released fix to address these vulnerabilities. Refer to MFSA 2019-08 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-08)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-07: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-07)
MFSA2019-07: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-07)
MFSA2019-08: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-08)
MFSA2019-08: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-08)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2019-9791
Description: Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR - The Exploit-DB Ref : 46613
Link: http://www.exploit-db.com/exploits/46613

Reference: CVE-2019-9792
Description: Spidermonkey - IonMonkey Leaks JS_OPTIMIZED_OUT Magic Value to Script - The Exploit-DB Ref : 46939
Link: http://www.exploit-db.com/exploits/46939

exploitdb

Reference: CVE-2019-9792
Description: Spidermonkey - IonMonkey Leaks JS_OPTIMIZED_OUT Magic Value to Script
Link: https://www.exploit-db.com/exploits/46939

Reference: CVE-2019-9791
Description: Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR
Link: https://www.exploit-db.com/exploits/46613

nvd

Reference: CVE-2019-9792
Description: The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
Link: http://packetstormsecurity.com/files/153106/Spidermonkey-IonMonkey-JS_OPTIMIZED_OUT-Value-Leak.html

Reference: CVE-2019-9792
Description: The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1532599

Reference: CVE-2019-9807
Description: When arbitrary text is sent over an FTP connection and a page reload is initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1362050

Reference: CVE-2019-9809
Description: If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1282430

Reference: CVE-2019-9791
Description: The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1530958

packetstorm

Reference: CVE-2019-9792
Description: Spidermonkey IonMonkey JS_OPTIMIZED_OUT Value Leak
Link: https://packetstormsecurity.com/files/153106/Spidermonkey-IonMonkey-JS_OPTIMIZED_OUT-Value-Leak.html

Reference: CVE-2019-9791
Description: SpiderMonkey IonMonkey Type Confusion
Link: https://packetstormsecurity.com/files/152266/SpiderMonkey-IonMonkey-Type-Confusion.html

0day.today

Reference: CVE-2019-9792
Description: Spidermonkey IonMonkey JS_OPTIMIZED_OUT Value Leak Exploit
Link: https://0day.today/exploit/32814

Reference: CVE-2019-9791
Description: Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR
Link: https://0day.today/exploit/32433

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-08,MFSA2020-09)

| | |
|---|---|
| QID: | 372445 |
| Category: | Local |
| Associated CVEs: | CVE-2020-6805, CVE-2020-6806, CVE-2020-6807, CVE-2020-6808, CVE-2020-6809, CVE-2020-6810, CVE-2020-6811, CVE-2019-20503, CVE-2020-6812, CVE-2020-6813, CVE-2020-6814, CVE-2020-6815 |
| Vendor Reference: | MFSA2020-08, MFSA2020-09 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2020-6805: Use-after-free when removing data about origins
CVE-2020-6806: BodyStream::OnInputStreamReady was missing protections against state confusion
CVE-2020-6807: Use-after-free in cubeb during stream destruction
CVE-2020-6808: URL Spoofing via javascript: URL
CVE-2020-6809: Web Extensions with the all-urls permission could access local files
CVE-2020-6810: Focusing a popup while in fullscreen could have obscured the fullscreen notification
CVE-2020-6811: Devtools' 'Copy as cURL' feature did not fully escape website-controlled data, potentially leading to command injection
CVE-2019-20503: Out of bounds reads in sctp_load_addresses_from_init
CVE-2020-6812: The names of AirPods with personally identifiable information were exposed to websites with camera or microphone permission
CVE-2020-6813: @import statements in CSS could bypass the Content Security Policy nonce feature
CVE-2020-6814: Memory safety bugs fixed in Firefox 74 and Firefox ESR 68.6
CVE-2020-6815: Memory and script safety bugs fixed in Firefox 74
Affected Products :
Prior to Firefox 74, Firefox ESR 68.6

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-08 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-08/)
MFSA2020-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-09/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-08 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-08/)
MFSA2020-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-09/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-20503
Description: usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.
Link: https://bugs.chromium.org/p/project-zero/issues/detail?id=1992

Reference: CVE-2020-6811
Description: The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as Curl' feature and pasted the command into a terminal, it could have resulted in command injection and

arbitrary command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1607742

packetstorm

Reference: CVE-2020-6806
Description: Firefox js::ReadableStreamCloseInternal Out-Of-Bounds Access
Link: https://packetstormsecurity.com/files/157524/Firefox-js-ReadableStreamCloseInternal-Out-Of-Bounds-Access.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-11)

| | |
|---|---|
| QID: | 372481 |
| Category: | Local |
| Associated CVEs: | CVE-2020-6819, CVE-2020-6820 |
| Vendor Reference: | MFSA2020-11 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2020-6819: Use-after-free while running the nsDocShell destructor
CVE-2020-6820: Use-after-free when handling a ReadableStream
Affected Products:
Prior to Firefox 74.0.1, Firefox ESR 68.6.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-11 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-11 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

cisa-kev

Reference: CVE-2020-6819
Description: Mozilla Firefox 74 and Firefox ESR 68.6 nsDocShell vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2020-6820
Description: Mozilla Firefox 74 and Firefox ESR 68.6 ReadableStream vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2020-6819
Description: Mozilla Firefox Use-after-free while running the nsDocShell destructor
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2020-6820

Description: Mozilla Firefox Use-after-free when handling a ReadableStream
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-12,MFSA2020-13)

| | |
|---|---|
| QID: | 372490 |
| Category: | Local |
| Associated CVEs: | CVE-2020-6821, CVE-2020-6822, CVE-2020-6823, CVE-2020-6824, CVE-2020-6825, CVE-2020-6826, CVE-2020-6827, CVE-2020-6828 |
| Vendor Reference: | MFSA2020-12, MFSA2020-13 |
| Bugtraq ID: | - |
| Service Modified: | 05/07/2020 |
| 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.
CVE-2020-6821: Uninitialized memory could be read when using the WebGL copyTexSubImage method
CVE-2020-6822: Out of bounds write in GMPDecodeData when processing large images
CVE-2020-6823: Malicious Extension could obtain auth codes from OAuth login flows
CVE-2020-6824: Generated passwords may be identical on the same site between separate private browsing sessions
CVE-2020-6825: Memory safety bugs fixed in Firefox 75 and Firefox ESR 68.7
CVE-2020-6826: Memory safety bugs fixed in Firefox 75
CVE-2020-6827: Custom Tabs in Firefox for Android could have the URI spoofed
CVE-2020-6828: Preference overwrite via crafted Intent from malicious Android application
Affected Products:

Prior to Firefox 75 , Firefox ESR 68.7

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-12 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-12/)
MFSA2020-13 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-13/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-12 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-12/)
MFSA2020-13 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-13/)

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 1.7.0.0

4 Mozilla Firefox/Thunderbird/SeaMonkey Arbitrary Code Execution Vulnerability

| | |
|---|---|
| QID: | 372650 |
| Category: | Local |
| Associated CVEs: | CVE-2013-0787 |
| Vendor Reference: | mfsa2013-29 |
| Bugtraq ID: | - |
| Service Modified: | 08/05/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Affected Versions:
Mozilla Firefox before 19.0.2
Firefox ESR 17.x prior to 17.0.4
Thunderbird prior to 17.0.4
Thunderbird ESR 17.x prior to 17.0.4
SeaMonkey prior to 2.16.1

IMPACT:

Successful exploitation could allow remote attackers to execute arbitrary code via vectors involving an execCommand call.

SOLUTION:

Kindly refer to mfsa2013-29 (https://www.mozilla.org/en-US/security/advisories/mfsa2013-29/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2013-29 (https://www.mozilla.org/en-US/security/advisories/mfsa2013-29/)

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  1.7.0.0

### 4 Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities MFSA (2012-42 to 53 and 2012-55, 2012-56 )

| | |
|---|---|
| QID: | 372654 |
| Category: | Local |
| Associated CVEs: | CVE-2012-1948, CVE-2012-1951, CVE-2012-1952, CVE-2012-1953, CVE-2012-1954, CVE-2012-1955, CVE-2012-1957, CVE-2012-1958, CVE-2012-1959, CVE-2012-1961, CVE-2012-1962, CVE-2012-1963, CVE-2012-1967, CVE-2012-1949, CVE-2012-1960, CVE-2012-1950, CVE-2012-1965, CVE-2012-1966, CVE-2012-1964 |
| Vendor Reference: | MFSA 2012-42, MFSA 2012-43, MFSA 2012-44, MFSA 2012-45, MFSA 2012-46, MFSA 2012-47, MFSA 2012-48, MFSA 2012-49, MFSA 2012-50, MFSA 2012-51, MFSA 2012-52, MFSA 2012-53, MFSA 2012-54, MFSA 2012-55, MFSA 2012-56 |
| Bugtraq ID: | - |
| Service Modified: | 06/03/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.

Affected Versions:
Firefox ESR 10.x prior to 10.0.6
Thunderbird ESR 10.x prior to 10.0.6
SeaMonkey prior to 2.11

IMPACT:

Successful exploitation could allows remote attackers to execute arbitrary JavaScript code with improper privileges via a javascript: URL.

SOLUTION:

Kindly refer to mfsa2012-56 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-56/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2012-56 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-56/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2012-19)

| | |
|---|---|
| QID: | 372655 |
| Category: | Local |
| Associated CVEs: | CVE-2012-0461, CVE-2012-0462, CVE-2012-0463, CVE-2012-0464 |
| Vendor Reference: | MFSA 2012-19 |
| Bugtraq ID: | - |
| Service Modified: | 06/04/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Affected versions:
Mozilla Firefox prior to 3.6.28 and 4.x through 10.0
Firefox ESR 10.x before 10.0.3
Thunderbird before 3.1.20 and 5.0 through 10.0
Thunderbird ESR 10.x before 10.0.3
SeaMonkey before 2.8

IMPACT:

Successful exploitation could allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

SOLUTION:

Kindly refer to mfsa2012-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-19/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2012-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-19/)

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 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-20, MFSA2020-21)

| | |
|---|---|
| QID: | 372825 |
| Category: | Local |
| Associated CVEs: | CVE-2020-12399, CVE-2020-12405, CVE-2020-12406, CVE-2020-12407, CVE-2020-12408, CVE-2020-12409, CVE-2020-12411, CVE-2020-12410 |
| Vendor Reference: | MFSA2020-20, MFSA2020-21 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2020-12399: Timing attack on DSA signatures in NSS library
CVE-2020-12405: Use-after-free in SharedWorkerService
CVE-2020-12406: JavaScript type confusion with NativeTypes
CVE-2020-12407: WebRender leaking GPU memory when using border-image CSS directive
CVE-2020-12408: URL spoofing when using IP addresses
CVE-2020-12409: URL spoofing with unicode characters
CVE-2020-12410: Memory safety bugs fixed in Firefox 77 and Firefox ESR 68.9
CVE-2020-12411: Memory safety bugs fixed in Firefox 77
Affected products:
Prior to Firefox 77
Prior to Firefox ESR 68.9

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/)MFSA2020-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/)
MFSA2020-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-12405
Description: When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1631618

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities(MFSA2020-24,MFSA2020-25)

| | |
|---|---|
| QID: | 373103 |
| Category: | Local |
| Associated CVEs: | CVE-2020-12415, CVE-2020-12416, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12402, CVE-2020-12421, CVE-2020-12422, CVE-2020-12423, CVE-2020-12424, CVE-2020-12425, CVE-2020-12426 |
| Vendor Reference: | MFSA2020-24, MFSA2020-25 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
Affected by Following vulnerabilities:
CVE-2020-12415: AppCache manifest poisoning due to url encoded character processing.
CVE-2020-12416: Use-after-free in WebRTC VideoBroadcaster.
CVE-2020-12417: Memory corruption due to missing sign-extension for ValueTags on ARM64.
CVE-2020-12418: Information disclosure due to manipulated URL object.
CVE-2020-12419: Use-after-free in nsGlobalWindowInner.
CVE-2020-12420: Use-After-Free when trying to connect to a STUN server.
CVE-2020-12402: RSA Key Generation vulnerable to side-channel attack.
CVE-2020-12421: Add-On updates did not respect the same certificate trust rules as software updates.
CVE-2020-12422: Integer overflow in nsJPEGEncoder::emptyOutputBuffer.
CVE-2020-12423: DLL Hijacking due to searching %PATH% for a library.
CVE-2020-12424: WebRTC permission prompt could have been bypassed by a compromised content process.
CVE-2020-12425: Out of bound read in Date.parse().
CVE-2020-12426: Memory safety bugs fixed in Firefox 78.
Affected Products :
Prior to Firefox 78
Prior to Firefox ESR 68.10

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/)MFSA2020-25 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/)
MFSA2020-25 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-12426
Description: Mozilla developers and community members reported memory safety bugs present in Firefox 77. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 78.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1608068%2C1609951%2C1631187%2C1637682

Reference: CVE-2020-12416
Description: A VideoStreamEncoder may have been freed in a race condition with VideoBroadcaster::AddOrUpdateSink, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1639734

Reference: CVE-2020-12417
Description: Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1640737

Reference: CVE-2020-12420
Description: When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1643437

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-30)

| | |
|---|---|
| QID: | 373320 |
| Category: | Local |
| Associated CVEs: | CVE-2020-15652, CVE-2020-6514, CVE-2020-15655, CVE-2020-15653, CVE-2020-6463, CVE-2020-15656, CVE-2020-15658, CVE-2020-15657, CVE-2020-15654, CVE-2020-15659 |
| Vendor Reference: | MFSA2020-30 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.
Firefox is found to be vulnerable to the following:
CVE-2020-15652: Potential leak of redirect targets when loading scripts in a worker
CVE-2020-6514: WebRTC data channel leaks internal address to peer
CVE-2020-15655: Extension APIs could be used to bypass Same-Origin Policy
CVE-2020-15653: Bypassing iframe sandbox when allowing popups
CVE-2020-6463: Use-after-free in ANGLE gl::Texture::onUnbindAsSamplerTexture
CVE-2020-15656: Type confusion for special arguments in IonMonkey
CVE-2020-15658: Overriding file type when saving to disk
CVE-2020-15657: DLL hijacking due to incorrect loading path
CVE-2020-15654: Custom cursor can overlay user interface
CVE-2020-15659: Memory safety bugs fixed in Firefox 79

Affected Versions:
versions prior to Firefox 79

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to
MFSA2020-30 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-30 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd
Reference: CVE-2020-6514
Description: Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.
Link: https://crbug.com/1076703

Reference: CVE-2020-6514
Description: Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to

potentially exploit heap corruption via a crafted SCTP stream.

Link: http://packetstormsecurity.com/files/158697/WebRTC-usrsctp-Incorrect-Call.html

0day.today

Reference: CVE-2020-6514

Description: WebRTC usrsctp Incorrect Call Vulnerability

Link: https://0day.today/exploit/34769

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 MozillaFirefox Multiple Vulnerabilities (MFSA2020-36)

| | |
|---|---|
| QID: | 373388 |
| Category: | Local |
| Associated CVEs: | CVE-2020-15663, CVE-2020-15664, CVE-2020-12401, CVE-2020-6829, CVE-2020-12400, CVE-2020-15665, CVE-2020-15666, CVE-2020-15667, CVE-2020-15668, CVE-2020-15670 |
| Vendor Reference: | MFSA2020-36 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2020-15663: Downgrade attack on the Mozilla Maintenance Service could have resulted in escalation of privilege

CVE-2020-15664: Attacker-induced prompt for extension installation

CVE-2020-12401: Timing-attack on ECDSA signature generation

CVE-2020-6829: P-384 and P-521 vulnerable to an electro-magnetic side channel attack on signature generation

CVE-2020-12400: P-384 and P-521 vulnerable to a side channel attack on modular inversion

CVE-2020-15665: Address bar not reset when choosing to stay on a page after the beforeunload dialog is shown

CVE-2020-15666: MediaError message property leaks cross-origin response status

CVE-2020-15667: Heap overflow when processing an update file

CVE-2020-15668: Data Race when reading certificate information

CVE-2020-15670: Memory safety bugs fixed in Firefox 80 and Firefox ESR 78.2
Affected Products : Prior to Firefox 80

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-36 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-36)
Patch:

Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-36: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2020-36)
MFSA2020-36: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2020-36)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-15665
Description: Firefox did not reset the address bar after the beforeunload dialog was shown if the user chose to remain on the page. This could have resulted in an incorrect URL being shown when used in conjunction with other unexpected browser behaviors. This vulnerability affects Firefox < 80.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1651636

Reference: CVE-2020-15666
Description: When trying to load a non-video in an audio/video context the exact status code (200, 302, 404, 500, 412, 403, etc.) was disclosed via the MediaError Message. This level of information leakage is inconsistent with the standardized onerror/onsuccess disclosure and can lead to inferring login status to services or device discovery on a local network among other attacks. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1450853

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities(MFSA2020-42)

| | |
|---|---|
| QID: | 373490 |
| Category: | Local |
| Associated CVEs: | CVE-2020-15675, CVE-2020-15677, CVE-2020-15676, CVE-2020-15678, CVE-2020-15673, CVE-2020-15674 |
| Vendor Reference: | MFSA2020-42 |
| Bugtraq ID: | - |
| Service Modified: | 10/22/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.
Firefox is found to be vulnerable to the following:
CVE-2020-15675: Use-After-Free in WebGL.
CVE-2020-15677: Download origin spoofing via redirect.
CVE-2020-15676: XSS when pasting attacker-controlled data into a contenteditable element.
CVE-2020-15678: When recursing through layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free scenario.
CVE-2020-15673: Memory safety bugs fixed in Firefox 81.
CVE-2020-15674: Memory safety bugs fixed in Firefox 81.
Affected Versions:
versions prior to Firefox 81

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to
MFSA2020-42 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-42 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/)

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  1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-50)

| | |
|---|---|
| QID: | 374166 |
| Category: | Local |
| Associated CVEs: | CVE-2020-26951, CVE-2020-26952, CVE-2020-16012, CVE-2020-26953, CVE-2020-26954, CVE-2020-26955, CVE-2020-26956, CVE-2020-26957, CVE-2020-26958, CVE-2020-26959, CVE-2020-26960, CVE-2020-15999, CVE-2020-26961, CVE-2020-26962, CVE-2020-26963, CVE-2020-26964, CVE-2020-26965, CVE-2020-26966, CVE-2020-26967, CVE-2020-26968, CVE-2020-26969 |
| Vendor Reference: | MFSA2020-50 |
| Bugtraq ID: | - |
| Service Modified: | 08/26/2023 |
| 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.
CVE-2020-26951: Parsing mismatches could confuse and bypass security sanitizer for chrome privileged code
CVE-2020-26952: Out of memory handling of JITed, inlined functions could lead to a memory corruption
CVE-2020-16012: Variable time processing of cross-origin images during drawImage calls
CVE-2020-26953: Fullscreen could be enabled without displaying the security UI
CVE-2020-26954: Local spoofing of web manifests for arbitrary pages in Firefox for Android
CVE-2020-26955: Cookies set during file downloads are shared between normal and Private Browsing Mode in Firefox for Android
CVE-2020-26956: XSS through paste (manual and clipboard API)
CVE-2020-26957: OneCRL was not working in Firefox for Android
CVE-2020-26958: Requests intercepted through ServiceWorkers lacked MIME type restrictions
CVE-2020-26959: Use-after-free in WebRequestService
CVE-2020-26960: Potential use-after-free in uses of nsTArray
CVE-2020-15999: Heap buffer overflow in freetype
CVE-2020-26961: DoH did not filter IPv4 mapped IP Addresses
CVE-2020-26962: Cross-origin iframes supported login autofill
CVE-2020-26963: History and Location interfaces could have been used to hang the browser
CVE-2020-26964: Firefox for Android's Remote Debugging via USB could have been abused by untrusted apps on older versions of Android
CVE-2020-26965: Software keyboards may have remembered typed passwords
CVE-2020-26966: Single-word search queries were also broadcast to local network
CVE-2020-26967: Mutation Observers could break or confuse Firefox Screenshots feature
CVE-2020-26968: Memory safety bugs fixed in Firefox 83 and Firefox ESR 78.5
CVE-2020-26969: Memory safety bugs fixed in Firefox 83
Affected Products:
Prior to Firefox 83.0.0

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-50 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-50: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/)
MFSA2020-50: WIndows (https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-15999
Description: Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
Link: https://crbug.com/1139963

Reference: CVE-2020-15999
Description: Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
Link: https://googleprojectzero.blogspot.com/p/rca-cve-2020-15999.html

Reference: CVE-2020-16012
Description: Side-channel information leakage in graphics in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
Link: https://crbug.com/1088224

packetstorm

Reference: CVE-2020-15999
Description: FreeType Load_SBit_Png Heap Buffer Overflow
Link: https://packetstormsecurity.com/files/159754/FreeType-Load_SBit_Png-Heap-Buffer-Overflow.html

github-exploits

Reference: CVE-2020-15999
Description: Marmeus/CVE-2020-15999 exploit repository
Link: https://github.com/Marmeus/CVE-2020-15999

Reference: CVE-2020-15999
Description: marcinguy/CVE-2020-15999 exploit repository
Link: https://github.com/marcinguy/CVE-2020-15999

cisa-kev

Reference: CVE-2020-15999
Description: Google Chrome FreeType Memory Corruption
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2020-15999
Description: Google Chrome Heap buffer overflow in typescript Load_SBit_Png
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2020-15999
Type: Exploit
Platform: Win32,Script

Malware ID: CVE-2012-0159
Type: Exploit
Platform: Image

Malware ID: Generic
Type: Exploit
Platform: Win32,Binary

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-01)

| | |
|---|---|
| QID: | 374827 |
| Category: | Local |
| Associated CVEs: | CVE-2020-16044 |
| Vendor Reference: | MFSA2021-01 |
| Bugtraq ID: | - |
| Service Modified: | 01/13/2021 |
| 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.
CVE-2020-16044: Use-after-free write when handling a malicious COOKIE-ECHO SCTP chunk

Affected Products:
Prior to Firefox 84.0.2

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-01: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/)
MFSA2021-01: WIndows (https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/)

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  1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-03)

| | |
|---|---|
| QID: | 374918 |
| Category: | Local |
| Associated CVEs: | CVE-2021-23953, CVE-2021-23954, CVE-2021-23955, CVE-2021-23956, CVE-2021-23957, CVE-2021-23958, CVE-2021-23959, CVE-2021-23960, CVE-2021-23961, CVE-2021-23962, CVE-2021-23963, CVE-2021-23964, CVE-2021-23965 |
| Vendor Reference: | MFSA2021-03 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2021-23953: Cross-origin information leakage via redirected PDF requests
CVE-2021-23954: Type confusion when using logical assignment operators in JavaScript switch statements
CVE-2021-23955: Clickjacking across tabs through misusing requestPointerLock

CVE-2021-23956: File picker dialog could have been used to disclose a complete directory
CVE-2021-23957: Iframe sandbox could have been bypassed on Android via the intent URL scheme
CVE-2021-23958: Screen sharing permission leaked across tabs
CVE-2021-23959: Cross-Site Scripting in error pages on Firefox for Android
CVE-2021-23960: Use-after-poison for incorrectly redeclared JavaScript variables during GC
CVE-2021-23961: More internal network hosts could have been probed by a malicious webpage
CVE-2021-23962: Use-after-poison in nsTreeBodyFrame::RowCountChanged
CVE-2021-23963: Permission prompt inaccessible after asking for additional permissions
CVE-2021-23964: Memory safety bugs fixed in Firefox 85 and Firefox ESR 78.7
CVE-2021-23965: Memory safety bugs fixed in Firefox 85
Affected Products:
Prior to Firefox 85

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-03 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-03: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/)
MFSA2021-03: WIndows (https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-23956
Description: An ambiguous file picker design could have confused users who intended to select and upload a single file into uploading a whole directory. This was addressed by adding a new prompt. This vulnerability affects Firefox < 85.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1338637

Reference: CVE-2021-23965
Description: Mozilla developers reported memory safety bugs present in Firefox 84. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1670378%2C1673555%2C1676812%2C1678582%2C1684497

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-07)

| | |
|---|---|
| QID: | 375209 |
| Category: | Local |
| Associated CVEs: | CVE-2021-23969, CVE-2021-23970, CVE-2021-23968, CVE-2021-23974, CVE-2021-23971, CVE-2021-23972, CVE-2021-23975, CVE-2021-23973, CVE-2021-23979 |
| Vendor Reference: | MFSA2021-07 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
CVE-2021-23969: Content Security Policy violation report could have contained the destination of a redirect.
CVE-2021-23970: Multithreaded WASM triggered assertions validating separation of script domains.
CVE-2021-23968: Content Security Policy violation report could have contained the destination of a redirect.
CVE-2021-23974: noscript elements could have led to an HTML Sanitizer bypass.

CVE-2021-23971: A website's Referrer-Policy could have been be overridden, potentially resulting in the full URL being sent as a Referrer.
CVE-2021-23972: HTTP Auth phishing warning was omitted when a redirect is cached.
CVE-2021-23975: about:memory Measure function caused an incorrect pointer operation.
CVE-2021-23973: MediaError message property could have leaked information about cross-origin resources.
CVE-2021-23979: Memory safety bugs fixed in Firefox 86.
Affected Products:
Prior to Firefox ESR 86

IMPACT:

On successful exploitation it could allow to compromise integrity, availability and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-07 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2021-07 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-23979

Description: Mozilla developers reported memory safety bugs present in Firefox 85. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86.

Link:

https://bugzilla.mozilla.org/buglist.cgi?bug_id=1663222%2C1666607%2C1672120%2C1678463%2C1678927%2C1679560%2C1681297%2C1681684%

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-10)

| | |
|---|---|
| QID: | 375408 |
| Category: | Local |
| Associated CVEs: | CVE-2021-23981, CVE-2021-23982, CVE-2021-23983, CVE-2021-23984, CVE-2021-23985, CVE-2021-23986, CVE-2021-23987, CVE-2021-23988, CVE-2021-29955, CVE-2021-29951 |
| Vendor Reference: | MFSA2021-10 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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.
Affected Products:
Prior to Firefox 87

IMPACT:

On successful exploitation it could allow to compromise integrity, availability and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2021-29951
Description: Mozilla Windows Maintenance Service Weak DACL
Link: https://packetstormsecurity.com/files/162522/Mozilla-Windows-Maintenance-Service-Weak-DACL.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-16)

| | |
|---|---|
| QID: | 375478 |
| Category: | Local |
| Associated CVEs: | CVE-2021-23994, CVE-2021-23995, CVE-2021-23996, CVE-2021-23997, CVE-2021-23998, CVE-2021-23999, CVE-2021-24000, CVE-2021-24001, CVE-2021-24002, CVE-2021-29945, CVE-2021-29944, CVE-2021-29946, CVE-2021-29947 |
| Vendor Reference: | MFSA2021-16 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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.
Affected Products:
Prior to Firefox 88

IMPACT:

On successful exploitation it could allow to compromise integrity, availability and confidentiality.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-16 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-16 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-23999
Description: If a Blob URL was loaded through some unusual user interaction, it could have been loaded by the System Principal and granted additional privileges that should not be granted to web content. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1691153

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Race Condition Vulnerability (MFSA2021-20)

| | |
|---|---|
| QID: | 375542 |
| Category: | Local |
| Associated CVEs: | CVE-2021-29952 |
| Vendor Reference: | MFSA2021-20 |
| Bugtraq ID: | - |
| Service Modified: | 07/02/2021 |
| 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.
When Web Render components were destructed, a race condition could have caused undefined behavior, and Mozilla presumes that with enough effort may have been exploitable to run arbitrary code.
Affected Products:
Prior to Firefox 88.0.1

IMPACT:

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

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-20/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2021-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-20/)

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  1.7.0.0

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 2.0.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-23)

| | |
|---|---|
| QID: | 375606 |
| Category: | Local |
| Associated CVEs: | CVE-2021-29965, CVE-2021-29960, CVE-2021-29961, CVE-2021-29964, CVE-2021-29959, CVE-2021-29967, CVE-2021-29966 |
| Vendor Reference: | MFSA2021-23 |
| Bugtraq ID: | - |
| Service Modified: | 07/27/2021 |
| 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 89

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-23 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-23)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-23 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-23)

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 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-28)

| | |
|---|---|
| QID: | 375712 |
| Category: | Local |
| Associated CVEs: | CVE-2021-29970, CVE-2021-29971, CVE-2021-30547, CVE-2021-29972, CVE-2021-29973, CVE-2021-29974, CVE-2021-29975, CVE-2021-29976, CVE-2021-29977 |
| Vendor Reference: | MFSA2021-28 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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.
Affected Products:
Prior to Firefox 90

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-28 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-28)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2021-28 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-29970
Description: A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1709976

Reference: CVE-2021-29972
Description: A use-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library. Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. This vulnerability affects Firefox < 90.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1696816

Reference: CVE-2021-29975
Description: Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. This vulnerability affects Firefox < 90.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1713259

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-33)

| | |
|---|---|
| QID: | 375753 |
| Category: | Local |

| | |
|---|---|
| Associated CVEs: | CVE-2021-29986, CVE-2021-29981, CVE-2021-29988, CVE-2021-29983, CVE-2021-29984, CVE-2021-29980, CVE-2021-29987, CVE-2021-29985, CVE-2021-29982, CVE-2021-29989, CVE-2021-29990 |
| Vendor Reference: | MFSA2021-33 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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.
Affected Products:
Prior to Firefox 91.0.1

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-33 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-33)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2021-33 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-33/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-29980
Description: Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1722204

Reference: CVE-2021-29982
Description: Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. This vulnerability affects Firefox < 91 and Thunderbird < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1715318

Reference: CVE-2021-29985
Description: A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1722083

Reference: CVE-2021-29984
Description: Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1720031

Reference: CVE-2021-29986
Description: A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1696138

Reference: CVE-2021-29988
Description: Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1717922

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-38)

| | |
|---|---|
| QID: | 375833 |
| Category: | Local |
| Associated CVEs: | CVE-2021-38491, CVE-2021-38492, CVE-2021-38493, CVE-2021-38494 |
| Vendor Reference: | MFSA2021-38 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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.
Affected Products:
Prior to Firefox 92

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-38 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-38 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-38492

Description: When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1721107

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 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  2.0.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-13)

| | |
|---|---|
| QID: | 376519 |
| Category: | Local |
| Associated CVEs: | CVE-2022-28287, CVE-2022-24713, CVE-2022-28281, CVE-2022-28286, CVE-2022-28288, CVE-2022-1097, CVE-2022-28283, CVE-2022-28282, CVE-2022-28289, CVE-2022-28284, CVE-2022-28285 |
| Vendor Reference: | MFSA2022-13 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-1097: Use-after-free in NSSToken objects
CVE-2022-28281: Out of bounds write due to unexpected WebAuthN Extensions
CVE-2022-28282: Use-after-free in DocumentL10n::TranslateDocument
CVE-2022-28283: Missing security checks for fetching sourceMapURL
CVE-2022-28284: Script could be executed via svg's use element
CVE-2022-28285: Incorrect AliasSet used in JIT Codegen
CVE-2022-28286: iframe contents could be rendered outside the border
CVE-2022-28287: Text Selection could crash Firefox
CVE-2022-24713: Denial of Service via complex regular expressions
CVE-2022-28289: Memory safety bugs fixed in Firefox 99 and Firefox ESR 91.8
CVE-2022-28288: Memory safety bugs fixed in Firefox 99
Affected Products:
Prior to Firefox 99

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 MFSA2022-13 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-13 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-1097
Description: NSSToken objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1745667

Reference: CVE-2022-28281
Description: If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-14/

Reference: CVE-2022-28281
Description: If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28281
Description: If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1755621

Reference: CVE-2022-28281
Description: If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-15/

Reference: CVE-2022-28282
Description: By using a link with rel="localization" a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28282
Description: By using a link with rel="localization" a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1751609

Reference: CVE-2022-28282
Description: By using a link with rel="localization" a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-15/

Reference: CVE-2022-28282
Description: By using a link with rel="localization" a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-14/

Reference: CVE-2022-28285
Description: When generating the assembly code for MLoadTypedArrayElementHole, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.

Link: https://www.mozilla.org/security/advisories/mfsa2022-14/

Reference: CVE-2022-28285
Description: When generating the assembly code for MLoadTypedArrayElementHole, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-15/

Reference: CVE-2022-28285
Description: When generating the assembly code for MLoadTypedArrayElementHole, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28285
Description: When generating the assembly code for MLoadTypedArrayElementHole, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1756957

Reference: CVE-2022-28286
Description: Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28286
Description: Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1735265

Reference: CVE-2022-28286
Description: Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-15/

Reference: CVE-2022-28286
Description: Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.
Link: https://www.mozilla.org/security/advisories/mfsa2022-14/

Reference: CVE-2022-28283
Description: The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. This vulnerability affects Firefox < 99.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28283
Description: The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. This vulnerability affects Firefox < 99.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1754066

Reference: CVE-2022-28287
Description: In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. This vulnerability affects Firefox < 99.
Link: https://www.mozilla.org/security/advisories/mfsa2022-13/

Reference: CVE-2022-28287
Description: In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. This vulnerability affects Firefox < 99.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1741515

? github-exploits

Reference: CVE-2022-28281
Description: 0vercl0k/CVE-2022-28281 exploit repository
Link: https://github.com/0vercl0k/CVE-2022-28281

Reference: CVE-2022-28282
Description: Pwnrin/CVE-2022-28282 exploit repository
Link: https://github.com/Pwnrin/CVE-2022-28282

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-16)

| | |
|---|---|
| QID: | 376574 |
| Category: | Local |
| Associated CVEs: | CVE-2022-29918, CVE-2022-29916, CVE-2022-29910, CVE-2022-29914, CVE-2022-29909, CVE-2022-29917, CVE-2022-29915, CVE-2022-29911, CVE-2022-29912 |
| Vendor Reference: | MFSA2022-16 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-29914: Fullscreen notification bypass using popups
CVE-2022-29909: Bypassing permission prompt in nested browsing contexts
CVE-2022-29916: Leaking browser history with CSS variables
CVE-2022-29911: iframe Sandbox bypass
CVE-2022-29912: Reader mode bypassed SameSite cookies
CVE-2022-29910: Firefox for Android forgot HTTP Strict Transport Security settings
CVE-2022-29915: Leaking cross-origin redirect through the Performance API
CVE-2022-29917: Memory safety bugs fixed in Firefox 100 and Firefox ESR 91.9
CVE-2022-29918: Memory safety bugs fixed in Firefox 100
Affected Products:
Prior to Firefox 100

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 MFSA2022-16 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-16/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-16 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-16/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-29912
Description: Requests initiated through reader mode did not properly omit cookies with a SameSite attribute. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1692655

Reference: CVE-2022-29916
Description: Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1760674

Reference: CVE-2022-29916
Description: Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://www.mozilla.org/security/advisories/mfsa2022-17/

Reference: CVE-2022-29916
Description: Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://www.mozilla.org/security/advisories/mfsa2022-16/

Reference: CVE-2022-29916
Description: Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://www.mozilla.org/security/advisories/mfsa2022-18/

Reference: CVE-2022-29917
Description: Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1684739%2C1706441%2C1753298%2C1762614%2C1762620%2C1764778

Reference: CVE-2022-29915
Description: The Performance API did not properly hide the fact whether a request cross-origin resource has observed redirects. This vulnerability affects Firefox < 100.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1751678

Reference: CVE-2022-29910
Description: When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings.*Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 100.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1757138

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-19)

| | |
|---|---|
| QID: | 376625 |
| Category: | Local |
| Associated CVEs: | CVE-2022-1802, CVE-2022-1529 |
| Vendor Reference: | MFSA2022-19 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-1802: Prototype pollution in Top-Level Await implementation
CVE-2022-1529: Untrusted input used in JavaScript object indexing, leading to prototype pollution
Affected Products:
Prior to Firefox 100.0.2

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. Refer to MFSA2022-19 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-19 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2022-1802
Description: mistymntncop/CVE-2022-1802 exploit repository
Link: https://github.com/mistymntncop/CVE-2022-1802

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-20)

| | |
|---|---|
| QID: | 376643 |
| Category: | Local |
| Associated CVEs: | CVE-2022-31747, CVE-2022-31743, CVE-2022-31738, CVE-2022-31744, CVE-2022-31748, CVE-2022-31740, CVE-2022-31739, CVE-2022-31736, CVE-2022-31741, CVE-2022-31745, CVE-2022-1919, CVE-2022-31742, CVE-2022-31737 |
| Vendor Reference: | MFSA2022-20 |
| 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-2022-31736: Cross-Origin resource's length leaked
CVE-2022-31737: Heap buffer overflow in WebGL
CVE-2022-31738: Browser window spoof using fullscreen mode
CVE-2022-31739: Attacker-influenced path traversal when saving downloaded files
CVE-2022-31740: Register allocation problem in WASM on arm64
CVE-2022-31741: Uninitialized variable leads to invalid memory read
CVE-2022-31742: Querying a WebAuthn token with a large number of allowCredential entries may have leaked cross-origin information
CVE-2022-31743: HTML Parsing incorrectly ended HTML comments prematurely
CVE-2022-31744: CSP bypass enabling stylesheet injection
CVE-2022-31745: Incorrect Assertion caused by unoptimized array shift operations
CVE-2022-1919: Memory Corruption when manipulating webp images
CVE-2022-31747: Memory safety bugs fixed in Firefox 101 and Firefox ESR 91.10
CVE-2022-31748: Memory safety bugs fixed in Firefox 101
Affected Products:
Prior to Firefox 101

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 MFSA2022-20 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-20 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/)

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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-24)

| | |
|---|---|
| QID: | 376705 |
| Category: | Local |
| Associated CVEs: | CVE-2022-34477, CVE-2022-34480, CVE-2022-34484, CVE-2022-34468, CVE-2022-34483, CVE-2022-34475, CVE-2022-34479, CVE-2022-2200, CVE-2022-34469, CVE-2022-34481, CVE-2022-34474, CVE-2022-34476, CVE-2022-34473, CVE-2022-34470, CVE-2022-34472, CVE-2022-34478, CVE-2022-34482, CVE-2022-34471, CVE-2022-34485 |
| Vendor Reference: | MFSA2022-24 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-34479: A popup window could be resized in a way to overlay the address bar with web content
CVE-2022-34470: Use-after-free in nsSHistory
CVE-2022-34468: CSP sandbox header without `allow-scripts` can be bypassed via retargeted javascript: URI
CVE-2022-34482: Drag and drop of malicious image could have led to malicious executable and potential code execution
CVE-2022-34483: Drag and drop of malicious image could have led to malicious executable and potential code execution
CVE-2022-34476: ASN.1 parser could have been tricked into accepting malformed ASN.1
CVE-2022-34481: Potential integer overflow in ReplaceElementsAt
CVE-2022-34474: Sandboxed iframes could redirect to external schemes
CVE-2022-34469: TLS certificate errors on HSTS-protected domains could be bypassed by the user on Firefox for Android
CVE-2022-34471: Compromised server could trick a browser into an addon downgrade
CVE-2022-34472: Unavailable PAC file resulted in OCSP requests being blocked
CVE-2022-34478: Microsoft protocols can be attacked if a user accepts a prompt
CVE-2022-2200: Undesired attributes could be set as part of prototype pollution
CVE-2022-34480: Free of uninitialized pointer in lg_init
CVE-2022-34477: MediaError message property leaked information on cross-origin same-site pages
CVE-2022-34475: HTML Sanitizer could have been bypassed via same-origin script via use tags
CVE-2022-34473: HTML Sanitizer could have been bypassed via use tags
CVE-2022-34484: Memory safety bugs fixed in Firefox 102 and Firefox ESR 91.11
CVE-2022-34485: Memory safety bugs fixed in Firefox 102
Affected Products:
Prior to Firefox 102

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 MFSA2022-24 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-34484

Description: The Mozilla Fuzzing Team reported potential vulnerabilities present in Thunderbird 91.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.

Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1763634%2C1772651

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-28)

| | |
|---|---|
| QID: | 376758 |
| Category: | Local |
| Associated CVEs: | CVE-2022-2505, CVE-2022-36318, CVE-2022-36319, CVE-2022-36317, CVE-2022-36320, CVE-2022-36314, CVE-2022-36315, CVE-2022-36316 |
| Vendor Reference: | MFSA2022-28 |
| Bugtraq ID: | - |
| Service Modified: | 04/11/2023 |
| 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-2022-36319: Mouse Position spoofing with CSS transforms
CVE-2022-36317: Long URL would hang Firefox for Android
CVE-2022-36318: Directory indexes for bundled resources reflected URL parameters
CVE-2022-36314: Opening local .lnk files could cause unexpected network loads
CVE-2022-36315: Preload Cache Bypasses Subresource Integrity
CVE-2022-36316: Performance API leaked whether a cross-site resource is redirecting
CVE-2022-36320: Memory safety bugs fixed in Firefox 103
CVE-2022-2505: Memory safety bugs fixed in Firefox 103 and 102.1
Affected Products:
Prior to Firefox 103

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 MFSA2022-28 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-28 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/)

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 1.7.0.0

## 4 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-33)

| | |
|---|---|
| QID: | 376857 |
| Category: | Local |
| Associated CVEs: | CVE-2022-38473, CVE-2022-38472, CVE-2022-38474, CVE-2022-38478, CVE-2022-38477, CVE-2022-38475 |
| Vendor Reference: | MFSA2022-33 |
| Bugtraq ID: | - |
| Service Modified: | 01/01/2023 |
| 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-2022-38472: Address bar spoofing via XSLT error handling
CVE-2022-38473: Cross-origin XSLT Documents would have inherited the parent's permissions
CVE-2022-38474: Recording notification not shown when microphone was recording on Android
CVE-2022-38475: Attacker could write a value to a zero-length array
CVE-2022-38477: Memory safety bugs fixed in Firefox 104 and Firefox ESR 102.2
CVE-2022-38478: Memory safety bugs fixed in Firefox 104, Firefox ESR 102.2, and Firefox ESR 91.13
Affected Products:
Prior to Firefox 104

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 MFSA2022-33 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-33/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-33 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-33/)

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  1.7.0.0

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: | 01/05/2023 |
| 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-2022-40959: 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  1.7.0.0

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 1.7.0.0

### 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: | 06/01/2023 |
| 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 3.0.17 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 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  1.7.0.0

### 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  1.7.0.0

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: | 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-2023-25728: 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 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  1.7.0.0

## 4 Microsoft WinVerifyTrust Signature Validation Vulnerability

| | |
|---|---|
| QID: | 378332 |
| Category: | Local |
| Associated CVEs: | CVE-2013-3900 |
| Vendor Reference: | CVE-2013-3900 |
| Bugtraq ID: | - |
| Service Modified: | 06/15/2023 |
| 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:

cisa-alerts
Reference: CVE-2013-3900
Description: CISA Adds 15 Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2022/01/10/cisa-adds-15-known-exploited-vulnerabilities-catalog

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

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  1.7.0.0

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  1.7.0.0

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  1.7.0.0

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: | 07/13/2023 |
| 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  1.7.0.0

### 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  1.7.0.0

### 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  1.7.0.0

## 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: | 09/15/2023 |
| 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  1.7.0.0

### 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  1.7.0.0

4 Mozilla Firefox Multiple Vulnerabilities (MFSA2023-44)

| | |
|---|---|
| QID: | 378906 |
| Category: | Local |
| Associated CVEs: | CVE-2023-5217 |
| Vendor Reference: | MFSA2023-44 |
| Bugtraq ID: | - |
| Service Modified: | 10/29/2023 |
| 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-2023-5217: 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:

cisa-alerts

Reference: CVE-2023-5217
Description: CISA Adds One Known Exploited Vulnerability to Catalog
Link: https://cisa.gov/news-events/alerts/2023/10/02/cisa-adds-one-known-exploited-vulnerability-catalog

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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 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  1.7.0.0

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  1.7.0.0

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: | 09/12/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

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: | 08/02/2023 |
| 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 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 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-2023-32051, CVE-2023-36872 |
| 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 Microsoft .NET Framework Update for November 2023

| | |
|---|---|
| QID: | 92078 |
| Category: | Windows |
| Associated CVEs: | CVE-2023-36049, CVE-2023-36560 |
| Vendor Reference: | 5031989, 5032004, 5032007, 5032197, 5032199, 5032336, 5032337, 5032338, 5032339, 5032340, 5032344, 5032341, 5032342, 5032343, 5032186, 5032185 |
| Bugtraq ID: | - |
| Service Modified: | 12/19/2023 |
| 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:
5032004
5032336
5032337
5032197
5031989
5032343
5032342
5032344
5032186
5032341
5032185
5032340
5032007
5032199
5032339
5032338
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 Elevation of Privileges.

SOLUTION:

Customers are advised to refer to CVE-2023-36049 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36049), CVE-2023-36560 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36560) for more details pertaining to these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2023-36049 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36049)
CVE-2023-36560 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36560)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5032339 or KB5032338 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.web.dll Version is 4.8.9195.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.web.dll Version is 4.8.9195.0

### 3 Mozilla Suite, Firefox, and Thunderbird XPInstall Security Dialog Vulnerability

| | |
|---|---|
| QID: | 115392 |
| Category: | Local |
| Associated CVEs: | CVE-2004-0762 |
| Vendor Reference: | - |
| Bugtraq ID: | 10661,15495 |
| Service Modified: | 06/09/2009 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Vulnerabilities in Mozilla Suite (pre-1.7), Firefox (pre-0.9) and Thunderbird (pre-0.7) could facilitate tricking a user into installing XPI packages without seeing a dialog box.

IMPACT:

An attacker may trick a user into installing an XPI package that contains various malicious payloads.

SOLUTION:

Mozilla has released Mozilla 1.7 and Mozilla Firefox 0.9 to address this issue

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  Version is  0.8.0.0

### 3 Mozilla Firefox User Interface Dispatcher Null Pointer Dereference Denial of Service Vulnerability - Zero Day

| | |
|---|---|
| QID: | 115966 |
| Category: | Local |
| Associated CVEs: | CVE-2008-4324 |
| Vendor Reference: | - |
| Bugtraq ID: | 31476 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Mozilla Firefox is prone to a remote denial of service vulnerability.

IMPACT:

Successful exploitation may allow attackers to crash the affected browser, resulting in denial of service conditions.

SOLUTION:

There are currently no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2008-4324
Description: Mozilla Firefox 3.0.3 - User Interface Null Pointer Dereference Crash - The Exploit-DB Ref : 6614
Link: http://www.exploit-db.com/exploits/6614

exploitdb

Reference: CVE-2008-4324
Description: Mozilla Firefox 3.0.3 - User Interface Null Pointer Dereference Crash
Link: https://www.exploit-db.com/exploits/6614

nvd

Reference: CVE-2008-4324
Description: The user interface event dispatcher in Mozilla Firefox 3.0.3 on Windows XP SP2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a series of keypress, click, onkeydown, onkeyup, onmousedown, and onmouseup events. NOTE: it was later reported that Firefox 3.0.2 on Mac OS X 10.5 is also affected.
Link: http://www.securityfocus.com/bid/31476

Reference: CVE-2008-4324
Description: The user interface event dispatcher in Mozilla Firefox 3.0.3 on Windows XP SP2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a series of keypress, click, onkeydown, onkeyup, onmousedown, and onmouseup events. NOTE: it was later reported that Firefox 3.0.2 on Mac OS X 10.5 is also affected.
Link: http://securityreason.com/securityalert/4321

Reference: CVE-2008-4324
Description: The user interface event dispatcher in Mozilla Firefox 3.0.3 on Windows XP SP2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a series of keypress, click, onkeydown, onkeyup, onmousedown, and onmouseup events. NOTE: it was later reported that Firefox 3.0.2 on Mac OS X 10.5 is also affected.
Link: http://www.secniche.org/moz303/index.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 0.8.0.0

## 3 Mozilla Firefox Information stealing via local shortcut files Vulnerability

| | |
|---|---|
| QID: | 115980 |
| Category: | Local |
| Associated CVEs: | CVE-2008-4582 |
| Vendor Reference: | MFSA2008-47 |
| Bugtraq ID: | 31747,31611 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox contains a vulnerability that allows attackers to violate the same-origin policy. The issue is caused due to the application failing to properly enforce the same-origin policy. Specifically, HTML files opened from the local drive may access subframes opened from local internet shortcut files.
Firefox Versions 3.0.1 through 3.0.3 for Microsoft Windows are vulnerable.

IMPACT:

An attacker may create a malicious Web page that can access the properties of another domain. This may allow the attacker to obtain sensitive information or launch other attacks against a user of the browser.

SOLUTION:

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox (Firefox) (http://www.mozilla.com/firefox/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2008-4582
Description: Mozilla Firefox 3.0.3 - Internet Shortcut Same Origin Policy Violation - The Exploit-DB Ref : 32466
Link: http://www.exploit-db.com/exploits/32466

exploitdb
Reference: CVE-2008-4582
Description: Mozilla Firefox 3.0.3 - Internet Shortcut Same Origin Policy Violation
Link: https://www.exploit-db.com/exploits/32466

seebug
Reference: CVE-2008-4582
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-85750

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 0.8.0.0

### 3 Mozilla Firefox 2 Cross-Domain Data Theft Redirect Error Message Vulnerability

| | |
|---|---|
| QID: | 116099 |
| Category: | Local |
| Associated CVEs: | CVE-2008-5507 |
| Vendor Reference: | MFSA-2008-65 |
| Bugtraq ID: | 32882 |
| Service Modified: | 01/05/2009 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a Web browser application.
This security update addresses a vulnerability that was not correctly patched in the previous release of Mozilla Firefox 2.
A Web site could access a limited amount of data from a different domain by loading a same-domain JavaScript URL which redirects to an off-domain target resource containing data which is not parsable as JavaScript. Upon attempting to load the data as JavaScript a syntax error is generated that can reveal some of the file context via the window.onerror DOM API.
Mozilla Firefox Versions 2.0.0.19 and prior on Windows are affected.

IMPACT:

This issue could be used by a malicious Web site to steal private data from users who are authenticated on the redirected Web site.

SOLUTION:

Update to the latest version of Mozilla Firefox (http://www.mozilla.com/firefox/).
This update marks the final release and support for Mozilla Firefox 2. We strongly recommend that you upgrade to Mozilla Firefox 3.

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  Version is  0.8.0.0

### 3 Mozilla Firefox Nested "window.print()" Denial of Service Vulnerability

| | |
|---|---|
| QID: | 116262 |
| Category: | Local |
| Associated CVEs: | CVE-2009-0821 |
| Vendor Reference: | - |
| Bugtraq ID: | 33969 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
The browser is prone to a remote denial of service vulnerability that occurs when the browser parses a malicious Web page containing nested "window.print()" JavaScript functions. An attacker can exploit this issue by enticing an unsuspecting user to visit a malicious site.
Firefox Version 2.0.0.20 is vulnerable; other versions may also be affected.

IMPACT:

If this vulnerability is successfully exploited, it allows attackers to cause the affected browser to crash denying service to legitimate users.

SOLUTION:

There are no vendor-supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2009-0821
Description: Mozilla Firefox 2.0.x - Nested 'window.print()' Denial of Service - The Exploit-DB Ref : 32836
Link: http://www.exploit-db.com/exploits/32836

exploitdb

Reference: CVE-2009-0821
Description: Mozilla Firefox 2.0.x - Nested 'window.print()' Denial of Service
Link: https://www.exploit-db.com/exploits/32836

nvd

Reference: CVE-2009-0821
Description: Mozilla Firefox 2.0.0.20 and earlier allows remote attackers to cause a denial of service (application crash) via nested calls to the window.print function, as demonstrated by a window.print(window.print()) in the onclick attribute of an INPUT element.
Link: http://downloads.securityfocus.com/vulnerabilities/exploits/33969.html

Reference: CVE-2009-0821
Description: Mozilla Firefox 2.0.0.20 and earlier allows remote attackers to cause a denial of service (application crash) via nested calls to the window.print function, as demonstrated by a window.print(window.print()) in the onclick attribute of an INPUT element.
Link: http://www.securityfocus.com/bid/33969

seebug

Reference: CVE-2009-0821
Description: Mozilla Firefox 2.0.x Nested 'window.print()' Denial of Service Vulnerability
Link: https://www.seebug.org/vuldb/ssvid-86104

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 3 Mozilla Firefox and SeaMonkey Multiple Vulnerabilities (MFSA 2009-52 through MFSA 2009-64)

| | |
|---|---|
| QID: | 116565 |
| Category: | Local |
| Associated CVEs: | CVE-2009-3274, CVE-2009-3370, CVE-2009-3371, CVE-2009-3372, CVE-2009-3373, CVE-2009-3374, CVE-2009-3375, CVE-2009-3376, CVE-2009-3377, CVE-2009-3378, CVE-2009-3379, CVE-2009-3380, CVE-2009-3381, CVE-2009-3382, CVE-2009-3383 |
| Vendor Reference: | Mozilla Foundation Security Advisories |
| Bugtraq ID: | - |
| Service Modified: | 07/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation has released multiple advisories to address vulnerabilities in Firefox and SeaMonkey:
1) An information-disclosure vulnerability could allow attackers to obtain history content. The problem occurs because a malicious Web page could synthesize mouse movement and key-press events to auto-populate formfields with history entries. Information obtained may aid in further attacks.It affects Firefox. (CVE-2009-3370)
2) A vulnerability is caused by recursive creation of JavaScript web-workers. An attacker can exploit this issue to free object memory before it is used. This will likely cause denial of service conditions; arbitrary code execution is possible. It affects Firefox. (CVE-2009-3371)
3) An arbitrary-code-execution vulnerability stems from a flaw in parsing regular expressions used in Proxy Auto-configuration (PAC) files. An attacker can exploit this issue to crash a victim's browser and possibly run arbitrary code. It affects Firefox and SeaMonkey. (CVE-2009-3372)
4) A heap-based buffer-overflow vulnerability occurs in the image parser for GIF color maps. An attacker can exploit this issue to execute arbitrary code in the context of the victim running the affected browser. This issue affects Firefox and SeaMonkey. (CVE-2009-3373)
5) A privilege-escalation vulnerability affects the XPCOM utility 'XPCVariant::VariantDataToJS()' because it doubly-wraps objects before returning them to chrome callers. An attacker can exploit this issue to execute malicious JavaScript with chrome privileges. It affects Firefox. (CVE-2009-3374)
6) A local privilege-escalation vulnerability occurs because the browser uses predictable names when downloading and saving files to the downloads folder. An attacker with local access and with knowledge of a file that a victim intends to open with Download Manager could exploit this issue to execute a malicious file in the context of the victim running the affected browser. It affects Firefox. (CVE-2009-3274)
7) A heap-based buffer-overflow vulnerability occurs in the string-to-floating-point conversion routines. An attacker can exploit this issue by tricking an unsuspecting victim into viewing a malicious Web page containing specially crafted JavaScript. A successful exploit will allow arbitrary code to run on the victim's computer. It affects Firefox. (CVE-2009-1563)
8) A cross-domain information-disclosure vulnerability occurs because text within a selection on a webpage can be read by JavaScript in a different domain using the 'document.getSelection' function. It affects Firefox. (CVE-2009-3375)
9) A vulnerability occurs that could allow an attacker to obfuscate the name and file extension of a file to be downloaded. The problem occurs when the file contains a right-to-left override character (RTL) in the filename. It affects Firefox and SeaMonkey. (CVE-2009-3376)
10) A remote code-execution vulnerability affects the third-party 'liboggz' library used in Firefox. It can be exploited to cause the browser to crash; arbitrary code execution may also be possible. (CVE-2009-3377)
11) A remote code-execution vulnerability affects the third-party 'libvorbis' library used in Firefox. It can be exploited to cause the browser to crash; arbitrary code execution may also be possible. (CVE-2009-3379)
12) A remote code-execution vulnerability affects the third-party 'liboggplay' library used in Firefox. It can be exploited to cause the browser to crash; arbitrary code execution may also be possible. (CVE-2009-3378)
13) Multiple remote memory-corruption vulnerabilities affect Firefox. These issues can be exploited to cause the browser to crash; arbitrary code execution may also be possible. (CVE-2009-3380, CVE-2009-3381, CVE-2009-3382, CVE-2009-3383)
Mozilla Firefox versions prior to 3.5.4, 3.0.15 and Mozilla SeaMonkey versions prior to 2.0 are vulnerable.
Previously this was a private iDefense detection.

IMPACT:

Attackers can exploit these issues to obtain potentially sensitive information, execute arbitrary code, and conduct privilege escalation attacks.

SOLUTION:

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.15&os=win&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.15&os=linux&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA

2009-62,MFSA 2009-63,MFSA 2009-64: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.15&os=osx&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Windows (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.4&os=win&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Linux (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.4&os=linux&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Mac OS (Firefox)
(http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.4&os=osx&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0&os=win&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0&os=linux&lang=en-US)
MFSA 2009-52,MFSA 2009-53,MFSA 2009-54,MFSA 2009-55,MFSA 2009-56,MFSA 2009-57,MFSA 2009-58,MFSA 2009-59,MFSA 2009-60,MFSA 2009-61,MFSA 2009-62,MFSA 2009-63,MFSA 2009-64: Mac OS (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2009-3373
Description: Mozilla Firefox 3.5.3 / SeaMonkey 1.1.17 - 'libpr0n' .GIF Parser Heap Buffer Overflow - The Exploit-DB Ref : 33313
Link: http://www.exploit-db.com/exploits/33313

Reference: CVE-2009-3382
Description: Mozilla Firefox 3.0.14 - Remote Memory Corruption - The Exploit-DB Ref : 33314
Link: http://www.exploit-db.com/exploits/33314

exploitdb

Reference: CVE-2009-3373
Description: Mozilla Firefox 3.5.3 / SeaMonkey 1.1.17 - 'libpr0n' .GIF Parser Heap Buffer Overflow
Link: https://www.exploit-db.com/exploits/33313

Reference: CVE-2009-3382
Description: Mozilla Firefox 3.0.14 - Remote Memory Corruption
Link: https://www.exploit-db.com/exploits/33314

nvd

Reference: CVE-2009-3371
Description: Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by creating JavaScript web-workers recursively.
Link: http://www.mozilla.org/security/announce/2009/mfsa2009-54.html

seebug

Reference: CVE-2009-3373
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-86542

Reference: CVE-2009-3382
Description: Mozilla Firefox
Link: https://www.seebug.org/vuldb/ssvid-86543

0day.today

Reference: CVE-2009-3373
Description: Mozilla Firefox 3.5.4 - Local Color Map Exploit
Link: https://0day.today/exploit/21131

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 3 Mozilla Firefox Network Security Services Multiple Vulnerabilities

| | |
|---|---|
| QID: | 116573 |
| Category: | Local |
| Associated CVEs: | CVE-2009-2408 |
| Vendor Reference: | MFSA 2009-42 |
| Bugtraq ID: | - |
| Service Modified: | 08/16/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor. Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications.
The following security vulnerability has been reported in Mozilla Firefox, Thunderbird, SeaMonkey and NSS:
Mozilla Firefox before 3.0.13 / 3.5, Thunderbird 2.0.0.23, SeaMonkey 1.1.18 and NSS 3.12.3 do not properly handle a "DESCRIPTION" character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority. (CVE-2009-2408)
If a malicious person requested a certificate for a host name with an invalid null character in it most CAs would issue the certificate if the requester owned the domain specified after the null, while most SSL clients (browsers) ignored that part of the name and used the unvalidated part in front of the null. This made it possible for attackers to obtain certificates that would function for any site they wished to target.
Updates to resolve this issue are available.

IMPACT:

Successful exploitation of this vulnerability could allow attackers to intercept and potentially alter encrypted communication between the client and a server such as sensitive bank account transactions. This attack could also be used to serve malicious updates.

SOLUTION:

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-32: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=linux&lang=en-US)
MFSA 2010-32: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.4&os=linux&lang=en-US)
MFSA 2010-32: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.10&os=linux&lang=en-US)
MFSA 2010-32: Mac OS (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=osx&lang=en-US)
MFSA 2010-32: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.4&os=osx&lang=en-US)
MFSA 2010-32: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.10&os=osx&lang=en-US)
MFSA 2010-32: Windows (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=win&lang=en-US)
MFSA 2010-32: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.4&os=win&lang=en-US)
MFSA 2010-32: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.5.10&os=win&lang=en-US)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 3 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities (MFSA 2010-09, MFSA 2010-10, MFSA 2010-11, MFSA 2010-12, MFSA 2010-13, MFSA 2010-14, MFSA 2010-15)

| | |
|---|---|
| QID: | 117103 |
| Category: | Local |
| Associated CVEs: | CVE-2010-0164, CVE-2010-0165, CVE-2010-0166, CVE-2010-0167, CVE-2010-0170, CVE-2010-0171, CVE-2010-0168, CVE-2010-0169, CVE-2010-0172 |
| Vendor Reference: | MFSA 2010-09, MFSA 2010-10, MFSA 2010-11, MFSA 2010-12, MFSA 2010-13, MFSA 2010-14, MFSA 2010-15 |

| | |
|---|---|
| Bugtraq ID: | 38918,38921,38919,38944,38943 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to the following vulnerabilities:
A vulnerability exists in Mozilla applications that is caused due to a use-after-free error when handling "multipart/x-mixed-replace" images, which could allow attackers to crash an affected browser or execute arbitrary code.
A vulnerability exists in Mozilla applications that is caused due to an error when handling "window.location" objects, which could allow cross-origin bypass via third-party plugins.
A vulnerability exists in Mozilla applications that is caused due to a memory corruption errors in the browser engines when parsing malformed data, which could be exploited by attackers to crash a vulnerable browser or execute arbitrary code.
A vulnerability exists in Mozilla applications that is caused due to an error when using "addEventListener" and "setTimeout" on a wrapped object, which could allow cross-site scripting attacks.
A vulnerability exists in Mozilla applications that is caused due to an error when preloading images, which could allow cross-site request forgery attacks against certain add-ons.
A vulnerability exists in Mozilla applications that is caused due to an error when handling stylesheets used in remote XUL documents, which could allow a malicious Web site to pollute a user's XUL cache and change style attributes of the browser (e.g. font size and color).
A vulnerability exists in Mozilla applications that is caused due to the new asynchronous Authorization Prompt (HTTP username and password) not always being attached to the correct window, which could allow attackers to conduct phishing attacks.

IMPACT:

Successful exploitation allows attackers to  manipulate or disclose certain data, bypass security restrictions or compromise a vulnerable system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-09 (http://www.mozilla.org/security/announce/2010/mfsa2010-09.html), MFSA 2010-10 (http://www.mozilla.org/security/announce/2010/mfsa2010-10.html), MFSA 2010-11 (http://www.mozilla.org/security/announce/2010/mfsa2010-11.html), MFSA 2010-12 (http://www.mozilla.org/security/announce/2010/mfsa2010-12.html), MFSA 2010-13 (http://www.mozilla.org/security/announce/2010/mfsa2010-13.html), MFSA 2010-14 (http://www.mozilla.org/security/announce/2010/mfsa2010-14.html), MFSA 2010-15 (http://www.mozilla.org/security/announce/2010/mfsa2010-15.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-11: Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.2&os=win&lang=en-US)
MFSA 2010-11: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.2&os=linux&lang=en-US)
MFSA 2010-11: Windows (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.3&os=win&lang=en-US)
MFSA 2010-11: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.3&os=linux&lang=en-US)
MFSA 2010-11: Windows (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.3&os=win&lang=en-US)
MFSA 2010-11: Linux (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.3&os=linux&lang=en-US)
MFSA 2010-11: Mac OS (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.3&os=osx&lang=en-US)
MFSA 2010-11: Mac OS (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.2&os=osx&lang=en-US)
MFSA 2010-11: Mac OS (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.3&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2010-0164

Description: Use-after-free vulnerability in the imgContainer::InternalAddFrameHelper function in src/imgContainer.cpp in libpr0n in Mozilla Firefox 3.6 before 3.6.2 allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a multipart/x-mixed-replace animation in which the frames have different bits-per-pixel (bpp) values.

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=547143

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

3 Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA 2010-18, MFSA 2010-19, MFSA 2010-20, MFSA 2010-21, MFSA 2010-16, MFSA 2010-17)

| | |
|---|---|
| QID: | 117436 |
| Category: | Local |
| Associated CVEs: | CVE-2010-0174, CVE-2010-0175, CVE-2010-0176, CVE-2010-0177, CVE-2010-0178, CVE-2010-0179 |
| Vendor Reference: | MFSA 2010-16, MFSA 2010-17, MFSA 2010-18, MFSA 2010-19, MFSA 2010-20, MFSA 2010-21 |
| Bugtraq ID: | 39124 |
| Service Modified: | 08/04/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client, and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client and HTML editor.
The following security vulnerabilities have been reported in Mozilla Firefox, Thunderbird and SeaMonkey:
1) An error related to the select event handler for XUL tree items can be exploited to potentially execute arbitrary code.
2) An error related to the XMLHttpRequestSpy object can be exploited to execute arbitrary JavaScript code with chrome privileges.
Successful exploitation requires that the "Firebug" addon is installed.

IMPACT:

Successful exploitation allows attackers to manipulate or disclose certain data, bypass security restrictions or compromise a vulnerable system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-17 (http://www.mozilla.org/security/announce/2010/mfsa2010-17.html), MFSA 2010-18 (http://www.mozilla.org/security/announce/2010/mfsa2010-18.html), MFSA 2010-19 (http://www.mozilla.org/security/announce/2010/mfsa2010-19.html), MFSA 2010-20 (http://www.mozilla.org/security/announce/2010/mfsa2010-20.html), MFSA 2010-21 (http://www.mozilla.org/security/announce/2010/mfsa2010-21.html),MFSA 2010-16 (http://www.mozilla.org/security/announce/2010/mfsa2010-16.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.2&os=linux&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.4&os=linux&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Linux (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=linux&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.2&os=win&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Windows (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.4&os=win&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Windows (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=win&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Mac OS (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.4&os=osx&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Mac OS (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.2&os=osx&lang=en-US)
MFSA 2010-16,MFSA 2010-17,MFSA 2010-18,MFSA 2010-19,MFSA 2010-20,MFSA 2010-21: Mac OS (Seamonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=osx&lang=en-US)

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  1.7.0.0

### 3 Mozilla Firefox, Thunderbird, SeaMonkey Remote Vulnerabilities (MFSA 2010-26, MFSA 2010-27, MFSA 2010-28, MFSA 2010-29, MFSA 2010-30, MFSA 2010-31, MFSA 2010-32, MFSA 2010-33)

| | |
|---|---|
| QID: | 118139 |
| Category: | Local |

| | |
|---|---|
| Associated CVEs: | CVE-2010-1200, CVE-2010-1201, CVE-2010-1202, CVE-2010-1203, CVE-2010-0183, CVE-2010-1198, CVE-2010-1196, CVE-2010-1199, CVE-2010-1197, CVE-2008-5913 |
| Vendor Reference: | MFSA 2010-26, MFSA 2010-27, MFSA 2010-28, MFSA 2010-29, MFSA 2010-30, MFSA 2010-31, MFSA 2010-32, MFSA 2010-33 |
| Bugtraq ID: | 41050,41087,41103,41102,41090,41094,41099,41082 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation has released six security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird, and SeaMonkey.
These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, crash affected applications, and perform cross-site scripting attacks; other attacks may also be possible.
Affected Versions:
Firefox Versions prior to 3.6.4
Firefox Versions prior to 3.5.10
Thunderbird Versions prior to 3.0.5
SeaMonkey Versions prior to 2.0.5

IMPACT:

Successful exploitation allows attackers to manipulate or disclose certain data, bypass security restrictions or compromise a vulnerable system.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-26 (http://www.mozilla.org/security/announce/2010/mfsa2010-26.html), MFSA 2010-27 (http://www.mozilla.org/security/announce/2010/mfsa2010-27.html), MFSA 2010-28 (http://www.mozilla.org/security/announce/2010/mfsa2010-28.html), MFSA 2010-29 (http://www.mozilla.org/security/announce/2010/mfsa2010-29.html), MFSA 2010-30 (http://www.mozilla.org/security/announce/2010/mfsa2010-30.html),MFSA 2010-31 (http://www.mozilla.org/security/announce/2010/mfsa2010-31.html), MFSA 2010-32 (http://www.mozilla.org/security/announce/2010/mfsa2010-32.html), MFSA 2010-33 (http://www.mozilla.org/security/announce/2010/mfsa2010-33.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.4&os=win&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.4&os=linux&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Mac OS X (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.4&os=osx&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Mac OS X (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.5&os=osx&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Windows (Thunderbird) (http://www.mozillamessaging.com/thunderbird/download/?product=thunderbird-3.0.5&os=win&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.5&os=linux&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=linux&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=win&lang=en-US)
MFSA 2010-25,MFSA 2010-26,MFSA 2010-27,MFSA 2010-28,MFSA 2010-29,MFSA 2010-30,MFSA 2010-31,MFSA 2010-32,MFSA 2010-33: Mac OS X (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.5&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2010-1199
Description: Mozilla Firefox/Thunderbird/SeaMonkey - XSLT Integer Overflow - The Exploit-DB Ref : 34192
Link: http://www.exploit-db.com/exploits/34192

Reference: CVE-2010-1199
Description: Mozilla Firefox 3.6.3 - XSLT Sort Remote Code Execution - The Exploit-DB Ref : 14949
Link: http://www.exploit-db.com/exploits/14949

exploitdb

Reference: CVE-2010-1199
Description: Mozilla Firefox/Thunderbird/SeaMonkey - XSLT Integer Overflow

Link: https://www.exploit-db.com/exploits/34192

Reference: CVE-2010-1199
Description: Mozilla Firefox 3.6.3 - XSLT Sort Remote Code Execution
Link: https://www.exploit-db.com/exploits/14949

nvd
Reference: CVE-2010-1201
Description: Unspecified vulnerability in the browser engine in Mozilla Firefox 3.5.x before 3.5.10, Thunderbird before 3.0.5, and SeaMonkey before 2.0.5 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=524921

packetstorm
Reference: CVE-2010-1199
Description: Month Of Abysssec Undisclosed Bugs - Firefox XSLT Sort Code Execution
Link: https://packetstormsecurity.com/files/93712/Month-Of-Abysssec-Undisclosed-Bugs-Firefox-XSLT-Sort-Code-Execution.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 3 Mozilla Firefox, Thunderbird, SeaMonkey "nsIContentPolicy" Security Bypass Vulnerability (MFSA 2010-24)

| | |
|---|---|
| QID: | 118157 |
| Category: | Local |
| Associated CVEs: | CVE-2010-0182, CVE-2010-0173, CVE-2010-0181 |
| Vendor Reference: | MFSA 2010-24 |
| Bugtraq ID: | 39479 |
| Service Modified: | 08/03/2022 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client, and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Mozilla applications are prone to a security-bypass vulnerability.
Attackers can exploit this issue to bypass security policies that prevent certain resources from being loaded. This may aid in further attacks.
Versions prior to the following are vulnerable:
Firefox V3.6.2
Firefox V3.5.9
Thunderbird V3.0.4
SeaMonkey V2.0.4

IMPACT:

Attackers can exploit this issue to bypass security policies that prevent certain resources from being loaded.

SOLUTION:

Update to Mozilla Thunderbird 3.04:
For Windows Platform:
thunderbird-3.0.4 for windows (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/win32/en-US/Thunderbird%20Setup%203.0.4.exe)
For Mac OSX Platform:
thunderbird-3.0.4 for Mac OSX (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/mac/en-US/Thunderbird%203.0.4.dmg)
For Linux Platform
thunderbird-3.0.4 for linux (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/linux-i686/en-US/thunderbird-3.0.4.tar.bz2)
Update to Mozilla Firefox 3.6.2:
For Windows Platform:
firfox 3.6.2 for windows (http://download.mozilla.org/?product=firefox-3.6.2&os=win&lang=en-US)
For Mac OSX Platform:

Firefox 3.6.2 for Mac OSX (http://download.mozilla.org/?product=firefox-3.6.2&os=osx&lang=en-US)
For Linux Platform
Firefox 3.6.2 for Linux (http://download.mozilla.org/?product=firefox-3.6.2&os=linux&lang=en-US)
Update to Mozilla SeaMonkey 2.04:
For Windows Platform:
SeaMondey 2.04 for Windows (http://download.mozilla.org/?product=seamonkey-2.0.4&os=win&lang=en-US)
For Mac OSX Platform:
SeaMonkey 2.04 for Mac OSX (http://download.mozilla.org/?product=seamonkey-2.0.4&os=osx&lang=en-US)
For Linux Platform
SeaMonkey 2.04 for linux (http://download.mozilla.org/?product=seamonkey-2.0.4&os=linux&lang=en-US)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-24: Windows (Thunderbird) (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/win32/en-US/Thunderbird%20Setup%203.0.4.exe)
MFSA 2010-24: Mac OSX (Thunderbird ) (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/mac/en-US/Thunderbird%203.0.4.dmg)
MFSA 2010-24: Linux (Thunderbird) (http://releases.mozilla.org/pub/mozilla.org/thunderbird/releases/3.0.4/linux-i686/en-US/thunderbird-3.0.4.tar.bz2)
MFSA 2010-24: Windows (Firefox ) (http://download.mozilla.org/?product=firefox-3.6.2&os=win&lang=en-US)
MFSA 2010-24: Mac OSX (Firefox) (http://download.mozilla.org/?product=firefox-3.6.2&os=osx&lang=en-US)
MFSA 2010-24: Linux (Firefox) (http://download.mozilla.org/?product=firefox-3.6.2&os=linux&lang=en-US)
MFSA 2010-24: Windows (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=win&lang=en-US)
MFSA 2010-24: Mac OSX (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=osx&lang=en-US)
MFSA 2010-24: Linux (SeaMonkey) (http://download.mozilla.org/?product=seamonkey-2.0.4&os=linux&lang=en-US)

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  1.7.0.0

### 3 Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities (MFSA 2010-34 to MFSA 2010-47)

| | |
|---|---|
| QID: | 118277 |
| Category: | Local |
| Associated CVEs: | CVE-2010-1214, CVE-2010-0654, CVE-2010-1211, CVE-2010-1213, CVE-2010-2752, CVE-2010-2753, CVE-2010-2754, CVE-2010-1208, CVE-2010-1209, CVE-2010-2751 |
| Vendor Reference: | MFSA 2010-34, MFSA 2010-35, MFSA 2010-36, MFSA 2010-37, MFSA 2010-38, MFSA 2010-39, MFSA 2010-40, MFSA 2010-41, MFSA 2010-42, MFSA 2010-43, MFSA 2010-44, MFSA 2010-45, MFSA 2010-46, MFSA 2010-47 |
| Bugtraq ID: | - |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application, Thunderbird is a standalone mail and newsgroup client and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
The Mozilla Foundation has released multiple security advisories specifying various vulnerabilities in Firefox, Thunderbird, and SeaMonkey. The following issues have been reported:
1) Multiple errors in the browser engine can be exploited to corrupt memory and potentially execute arbitrary code.
2) A use-after-free error within the DOM attribute cloning routine can be exploited to execute arbitrary code.
3) A use-after-free error within the NodeIterator implementation can be exploited to execute arbitrary code.
4) An error within the handling of parameters when embedding plugin content can be exploited to execute arbitrary code.
5) An error when accessing a content object via SJOW from the chrome scope can be exploited to execute arbitrary JavaScript code with chrome privileges.
6) An error when handling certain CSS array values (e.g. when handling external font resources) can be exploited to execute arbitrary code.
7) An integer overflow when calculating ranges for nsTreeSelection can be exploited to trigger the use of an invalid pointer and execute arbitrary code.
8) An error when handling certain PNG images can be exploited to execute arbitrary code.
9) An error within the Web Worker method importScripts can be exploited to bypass the same-origin policy and disclose potentially sensitive information.
10) An error within the canvas element after rendering cross-origin data can be exploited to bypass the same-origin policy and disclose potentially sensitive information.
11) A weakness exists when handling undefined positions within various 8 bit character encodings, which can lead to characters disappearing from the text run. This can potentially be leveraged to conduct cross-site scripting attacks.
12) A weakness exists when handling certain redirect sequences and responses in combination with JavaScript and SSL/TLS, which can be exploited to spoof the location bar to indicate a secure page, although the current document was served via plaintext.
13) A weakness when handling certain CSS selectors can be exploited to disclose potentially sensitive information by injecting CSS selectors into a target page and

accessing the region between the selectors via e.g. the JavaScript "getComputedStyle()" API.
14) A vulnerability is caused due to the "window.onerror" handler being allowed to read the destination URL of a redirection. This can be exploited to e.g. disclose session-specific query parameters contained in a target URL by referencing a redirecting site via an HTML "script" tag.

IMPACT:

Successful exploitation allows attackers to manipulate or disclose certain data, bypass security restrictions or compromise a vulnerable system.

SOLUTION:

These issues have been fixed in Firefox 3.6.7 and later, Firefox 3.5.11 and later, SeaMonkey 2.0.6 and later, Thunderbird 3.0.6 and 3.1.1 and later.
The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-37 (http://www.mozilla.org/security/announce/2010/mfsa2010-37.html), MFSA 2010-38 (http://www.mozilla.org/security/announce/2010/mfsa2010-38.html), MFSA 2010-39 (http://www.mozilla.org/security/announce/2010/mfsa2010-39.html), MFSA 2010-40 (http://www.mozilla.org/security/announce/2010/mfsa2010-40.html), MFSA 2010-41 (http://www.mozilla.org/security/announce/2010/mfsa2010-41.html), MFSA 2010-42 (http://www.mozilla.org/security/announce/2010/mfsa2010-42.html),MFSA 2010-43 (http://www.mozilla.org/security/announce/2010/mfsa2010-43.html), MFSA 2010-44 (http://www.mozilla.org/security/announce/2010/mfsa2010-44.html), MFSA 2010-45 (http://www.mozilla.org/security/announce/2010/mfsa2010-45.html), MFSA 2010-46 (http://www.mozilla.org/security/announce/2010/mfsa2010-46.html), MFSA 2010-47 (http://www.mozilla.org/security/announce/2010/mfsa2010-47.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Windows (Firefox) (http://www.mozilla.com/products/download.html?product=firefox-3.6.7&os=win&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.7&os=osx&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.7&os=linux&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Windows (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.6&os=win&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Linux (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.6&os=linux&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Mac OS (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.6&os=osx&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Windows (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.6&os=win&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.6&os=linux&lang=en-US)
MFSA 2010-37,MFSA 2010-38,MFSA 2010-39,MFSA 2010-40,MFSA 2010-41,MFSA 2010-42,MFSA 2010-43,MFSA 2010-44,MFSA 2010-45,MFSA 2010-46,MFSA 2010-47:
Mac OS (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.0.6&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2010-1214
Description: Mozilla Firefox and SeaMonkey Plugin Parameters - Remote Buffer Overflow - The Exploit-DB Ref : 34358
Link: http://www.exploit-db.com/exploits/34358

Reference: CVE-2010-1214
Description: Mozilla Firefox 3.6.4 - 'Plugin' EnsureCachedAttrParamArrays Remote Code Execution - The Exploit-DB Ref : 15027
Link: http://www.exploit-db.com/exploits/15027

Reference: CVE-2010-2752
Description: Mozilla Firefox CSS - font-face Remote Code Execution - The Exploit-DB Ref : 15104
Link: http://www.exploit-db.com/exploits/15104

exploitdb

Reference: CVE-2010-1214
Description: Mozilla Firefox and SeaMonkey Plugin Parameters - Remote Buffer Overflow
Link: https://www.exploit-db.com/exploits/34358

Reference: CVE-2010-1214
Description: Mozilla Firefox 3.6.4 - 'Plugin' EnsureCachedAttrParamArrays Remote Code Execution
Link: https://www.exploit-db.com/exploits/15027

Reference: CVE-2010-2752
Description: Mozilla Firefox CSS - font-face Remote Code Execution
Link: https://www.exploit-db.com/exploits/15104

nvd

Reference: CVE-2010-0654
Description: Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, Thunderbird 3.0.x before 3.0.6 and 3.1.x before 3.1.1, and SeaMonkey before 2.0.6 permit cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote attackers to obtain sensitive information via a crafted document.
Link: http://code.google.com/p/chromium/issues/detail?id=9877

Reference: CVE-2010-2751
Description: The nsDocShell::OnRedirectStateChange function in docshell/base/nsDocShell.cpp in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, allows remote attackers to spoof the SSL security status of a document via vectors involving multiple requests, a redirect, and the history.back and history.forward JavaScript functions.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=536466

packetstorm

Reference: CVE-2010-2752
Description: Month Of Abysssec Undisclosed Bugs - Mozilla Firefox CSS Font-Face
Link: https://packetstormsecurity.com/files/94241/Month-Of-Abysssec-Undisclosed-Bugs-Mozilla-Firefox-CSS-Font-Face.html

Reference: CVE-2010-1214
Description: Month Of Abysssec Undisclosed Bugs - Firefox Plugin Parameter
Link: https://packetstormsecurity.com/files/93987/Month-Of-Abysssec-Undisclosed-Bugs-Firefox-Plugin-Parameter.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

3 Firefox and SeaMonkey Web Browser Clickjacking Vulnerability

| | |
|---|---|
| QID: | 118301 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 07/26/2010 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a Web browser application and SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Firefox and SeaMonkey are exposed to a Web Browser Clickjacking Vulnerability.
Affected Versions:
Firefox 3.6.7
SeaMonkey 2.0.6

IMPACT:

Successful exploitation allows attackers to execute script code without user's knowledge.

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:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

3 Mozilla Firefox NSS Certificate IP Address Wildcard Matching Vulnerability

| | |
|---|---|
| QID: | 118450 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 09/01/2010 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is an open source Web browser available for multiple Operating Systems.
Firefox is prone to a vulnerability caused by the use of vulnerable Network Security Services code.

IMPACT:

Successful exploitation allows malicious users to conduct spoofing attacks.

SOLUTION:

There are no vendor supplied patches available at this time. Reportedly, this will be fixed in the Firefox Versions after 3.6.9 and 3.5.12.

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 1.7.0.0

3 Mozilla Firefox Multiple Vulnerabilities (MFSA 2010-64 through MFSA 2010-72)

| | |
|---|---|
| QID: | 118614 |
| Category: | Local |
| Associated CVEs: | CVE-2010-3183, CVE-2010-3182, CVE-2010-3181, CVE-2010-3180, CVE-2010-3179, CVE-2010-3178, CVE-2010-3177, CVE-2010-3176, CVE-2010-3175, CVE-2010-3174, CVE-2010-3173 |
| Vendor Reference: | MSFA2010-63, MSFA2010-64, MSFA2010-65, MSFA2010-66, MSFA2010-67, MSFA2010-68, MSFA2010-69, MSFA2010-70, MSFA2010-71, MSFA2010-72 |
| Bugtraq ID: | 44144,44245,44243,44248,44251,44249,44252 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The Mozilla Foundation has released eight security advisories specifying vulnerabilities in Mozilla Firefox, Thunderbird, and SeaMonkey.
These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, crash affected applications, elevate privileges, and disclose potentially sensitive information; other attacks may also be possible.
These issues are fixed in:

Firefox 3.6.11
Firefox 3.5.14
Thunderbird 3.0.9
Thunderbird 3.1.5
SeaMonkey 2.0.9

IMPACT:

These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, crash affected applications, elevate privileges, and disclose potentially sensitive information; other attacks may also be possible.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details: MFSA 2010-64 (http://www.mozilla.org/security/announce/2010/mfsa2010-64.html), MFSA 2010-65 (http://www.mozilla.org/security/announce/2010/mfsa2010-65.html), MFSA 2010-66 (http://www.mozilla.org/security/announce/2010/mfsa2010-66.html), MFSA 2010-67 (http://www.mozilla.org/security/announce/2010/mfsa2010-67.html), MFSA 2010-68 (http://www.mozilla.org/security/announce/2010/mfsa2010-68.html), MFSA 2010-69 (http://www.mozilla.org/security/announce/2010/mfsa2010-69.html), MFSA 2010-70 (http://www.mozilla.org/security/announce/2010/mfsa2010-70.html), MFSA 2010-71 (http://www.mozilla.org/security/announce/2010/mfsa2010-71.html), MFSA 2010-72 (http://www.mozilla.org/security/announce/2010/mfsa2010-72.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Windows (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.11&os=win&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Windows (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.5&os=win&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Windows (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.9&os=win&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Linux (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.11&os=linux&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Linux (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.5&os=linux&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Linux (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.9&os=linux&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Mac OS (Firefox) (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6.11&os=osx&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Mac OS (Thunderbird) (http://www.mozillamessaging.com/en-US/thunderbird/download/?product=thunderbird-3.1.5&os=osx&lang=en-US)
MFSA 2010-64,MFSA 2010-65,MFSA 2010-66,MFSA 2010-67,MFSA 2010-68,MFSA 2010-69,MFSA 2010-70,MFSA 2010-71,MFSA 2010-72: Mac OS (Sea Monkey) (http://download.mozilla.org/?product=seamonkey-2.0.9&os=osx&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2010-3179
Description: Mozilla Firefox SeaMonkey 3.6.10 / Thunderbird 3.1.4 - 'document.write' Memory Corruption - The Exploit-DB Ref : 34881
Link: http://www.exploit-db.com/exploits/34881

exploitdb
Reference: CVE-2010-3179
Description: Mozilla Firefox SeaMonkey 3.6.10 / Thunderbird 3.1.4 - 'document.write' Memory Corruption
Link: https://www.exploit-db.com/exploits/34881

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 3 Mozilla Firefox Fraudulent SSL Certificate Issue (MFSA 2011-11)

| | |
|---|---|
| QID: | 119084 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | Mozilla Update |
| Bugtraq ID: | - |
| Service Modified: | 03/30/2011 |
| User Modified: | - |
| Edited: | No |

PCI Vuln: Yes

THREAT:

Firefox is a Web browser application.
Mozilla Firefox has been updated to blacklists a some HTTPS certificates.
Affected Versions:
Firefox versions prior to 3.5.18
Firefox 3.6.x versions prior to 3.6.16

IMPACT:

Attackers can exploit this issues to launch phishing attacks. Other attacks are also possible

SOLUTION:

The vendor has released an updates (Firefox 3.5.18, 3.6.16 and 4.0) to resolve this issue. For more information refer to vendor blog fraudulent certificates (http://blog.mozilla.com/security/2011/03/22/firefox-blocking-fraudulent-certificates/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Firefox 4.0: Windows (http://www.mozilla.com/products/download.html?product=firefox-4.0&os=win&lang=en-US)
Firefox 4.0: Mac OS X (http://www.mozilla.com/products/download.html?product=firefox-4.0&os=osx&lang=en-US)
Firefox 3.6.16: Windows (http://www.mozilla.com/products/download.html?product=firefox-3.6.16&os=win&lang=en-US)
Firefox 3.6.16: Mac OS X (http://www.mozilla.com/products/download.html?product=firefox-3.6.16&os=osx&lang=en-US)
Firefox 3.5.18: Windows (http://www.mozilla.com/products/download.html?product=firefox-3.5.18&os=win&lang=en-US)
Firefox 3.5.18: Mac OS X (http://www.mozilla.com/products/download.html?product=firefox-3.5.18&os=osx&lang=en-US)

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 1.7.0.0

### 3 Mozilla Firefox Thunderbird and SeaMonkey Fraudulent Digital Certificate Spoofing Vulnerability (MFSA2011-35)

| | |
|---|---|
| QID: | 119568 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | Mozilla Security Update, MFSA2011-35 |
| Bugtraq ID: | - |
| Service Modified: | 08/30/2011 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for multiple platforms.
Mozilla was informed about the issuance of at least one fraudulent SSL certificate for public websites belonging to Google, Inc. This is not a Firefox-specific issue, and the certificate has now been revoked by its issuer, DigiNotar.
Mozilla issued a update that will revoke trust in the DigiNotar root and protect users from this attack.
Affected Software:
Firefox Versions prior to 3.6.22 and 6.0.2.
Thunderbird Versions prior to 3.1.14 and 6.0.2
SeaMonkey Versions prior to 2.3.3

IMPACT:

Users on a compromised network could be directed to sites using a fraudulent certificate and mistake them for the legitimate sites. This could deceive them into revealing personal information such as usernames and passwords. It may also deceive users into downloading malware if they believe it is coming from a trusted site.

SOLUTION:

Vendor has released updated versions (Firefox 3.6.22 and 6.0.2, Thunderbird 3.1.14 and 6.0.2, SeaMonkey 2.3.3) to fix these issues. Refer to vendor advisory MFSA2011-035 (http://www.mozilla.org/security/announce/2011/mfsa2011-35.html) for more inforamation.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2011-35: Linux (Firefox 3.6.22) (http://www.mozilla.org/en-US/products/download.html?product=firefox-3.6.22&os=linux&lang=en-US)
MFSA2011-35: Linux (Firefox 6.0.2) (http://download.mozilla.org/?product=firefox-6.0.2&os=linux&lang=en-US)
MFSA2011-35: Linux (Thunderbird 3.1.14) (http://download.mozilla.org/?product=thunderbird-3.1.14&os=linux&lang=en-US)
MFSA2011-35: Linux (Thunderbird 6.0.2) (http://download.mozilla.org/?product=thunderbird-6.0.2&os=linux&lang=en-US)
MFSA2011-35: Linux (Seamonkey 2.3.3) (http://download.mozilla.org/?product=seamonkey-2.3.3&os=linux&lang=en-US)
MFSA2011-35: Mac OS X (Firefox 3.6.22) (http://www.mozilla.org/en-US/products/download.html?product=firefox-3.6.22&os=osx&lang=en-US)
MFSA2011-35: Mac OS X (Firefox 6.0.2) (http://download.mozilla.org/?product=firefox-6.0.2&os=osx&lang=en-US)
MFSA2011-35: Mac OS X (Thunderbird 3.1.14) (http://download.mozilla.org/?product=thunderbird-3.1.14&os=osx&lang=en-US)
MFSA2011-35: Mac OS X (Thunderbird 6.0.2) (http://download.mozilla.org/?product=thunderbird-6.0.2&os=osx&lang=en-US)
MFSA2011-35: Mac OS X (Seamonkey 2.3.3) (http://download.mozilla.org/?product=seamonkey-2.3.3&os=osx&lang=en-US)
MFSA2011-35: Windows (Firefox 3.6.22) (http://www.mozilla.org/en-US/products/download.html?product=firefox-3.6.22&os=win&lang=en-US)
MFSA2011-35: Windows (Firefox 6.0.2) (http://download.mozilla.org/?product=firefox-6.0.2&os=win&lang=en-US)
MFSA2011-35: Windows (Thunderbird 3.1.14) (http://download.mozilla.org/?product=thunderbird-3.1.14&os=win&lang=en-US)
MFSA2011-35: Windows (Thunderbird 6.0.2) (http://download.mozilla.org/?product=thunderbird-6.0.2&os=win&lang=en-US)
MFSA2011-35: Windows (Seamonkey 2.3.3) (http://download.mozilla.org/?product=seamonkey-2.3.3&os=win&lang=en-US)

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  1.7.0.0

## 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: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

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

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 2.0.0.0

3 Mozilla Firefox/SeaMonkey/Thunderbird Multiple Cross-Site Scripting Vulnerabilities (MFSA 2012-90)

QID: 120651

| | |
|---|---|
| Category: | Local |
| Associated CVEs: | CVE-2012-4196, CVE-2012-4194, CVE-2012-4195 |
| Vendor Reference: | MFSA2012-90 |
| Bugtraq ID: | 56306,56301,56302 |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Mozilla has fixed a number of issues related to the Location object in order to enhance overall security.
Affected Versions:
Firefox prior to 16.0.2
Firefox ESR prior to 10.0.10
Thunderbird prior to 16.0.2
Thunderbird ESR prior to 10.0.10
SeaMonkey prior to 2.13.2

IMPACT:

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

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following Mozilla Foundation security advisories for further details:
MFSA 2012-90 (http://www.mozilla.org/security/announce/2012/mfsa2012-90.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2012-90: OSX (Firefox 16.0.2) (http://download.mozilla.org/?product=firefox-16.0.2&os=osx&lang=en-US)
MFSA2012-90: OSX (Firefox ESR 10.0.10) (http://download.mozilla.org/?product=firefox-10.0.10esr&os=osx&lang=en-US)
MFSA2012-90: OSX (Thunderbird 16.0.2) (http://download.mozilla.org/?product=thunderbird-16.0.2&os=osx&lang=en-US)
MFSA2012-90: OSX (Thunderbird ESR 10.0.10) (http://download.mozilla.org/?product=thunderbird-10.0.10esr&os=osx&lang=en-US)
MFSA2012-90: OSX (SeaMonkey 2.13.2) (http://download.mozilla.org/?product=seamonkey-2.13.2&os=osx&lang=en-US)
MFSA2012-90: Windows (Firefox 16.0.2) (http://download.mozilla.org/?product=firefox-16.0.2&os=win&lang=en-US)
MFSA2012-90: Windows (Firefox ESR 10.0.10) (http://download.mozilla.org/?product=firefox-10.0.10esr&os=win&lang=en-US)
MFSA2012-90: Windows (Thunderbird 16.0.2) (http://download.mozilla.org/?product=thunderbird-16.0.2&os=win&lang=en-US)
MFSA2012-90: Windows (Thunderbird ESR 10.0.10) (http://download.mozilla.org/?product=thunderbird-10.0.10esr&os=win&lang=en-US)
MFSA2012-90: Windows (SeaMonkey 2.13.2) (http://download.mozilla.org/?product=seamonkey-2.13.2&os=win&lang=en-US)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2012-4194
Description: Mozilla Firefox before 16.0.2, Firefox ESR 10.x before 10.0.10, Thunderbird before 16.0.2, Thunderbird ESR 10.x before 10.0.10, and SeaMonkey before 2.13.2 do not prevent use of the valueOf method to shadow the location object (aka window.location), which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via vectors involving a plugin.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=800666

Reference: CVE-2012-4196
Description: Mozilla Firefox before 16.0.2, Firefox ESR 10.x before 10.0.10, Thunderbird before 16.0.2, Thunderbird ESR 10.x before 10.0.10, and SeaMonkey before 2.13.2 allow remote attackers to bypass the Same Origin Policy and read the Location object via a prototype property-injection attack that defeats certain protection mechanisms for this object.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=802557

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 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 2.0.0.0

### 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: | 05/28/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 3 VLC Media Player Multiple Security Vulnerability

| | |
|---|---|
| QID: | 121324 |
| Category: | Local |
| Associated CVEs: | CVE-2013-3245, CVE-2013-1954 |
| Vendor Reference: | VLC Advisory, ,VLC Advisory |
| Bugtraq ID: | 61032,57333 |
| Service Modified: | 11/08/2023 |
| 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 application suffers from an Integer Overflow vulnerability. The vulnerability exist in libmkv_plugin.dll file which is used for parsing MKV files. This issue can be exploited to cause aa overflow via an MKV file with a specially crafted header.
Affected Versions:
The vulnerability is confirmed in version 2.0.7. Older versions up-to 2.0.0 are also vulnerable.
The application suffers from an Buffer Overflow vulnerability. The vulnerability exist in freetype renderer and HTML subtitle parser file which is used for parsing. This issue can be exploited to cause a overflow via a maliciously crafted file.
Affected Versions:
The vulnerability is confirmed in version 2.0.4. Older versions up-to 2.0.0 are also vulnerable.

The application suffers from an Buffer Overflow vulnerability. The vulnerability exist in ASF Demuxer which is used for parsing ASF files. This issue can be exploited to cause a overflow via an ASF file with a specially crafted header.
Affected Versions:
The vulnerability is confirmed in version 2.0.5. Older versions up-to 2.0.0 are also vulnerable.

IMPACT:

Successful exploitation of the vulnerabilities causes an Overflow that allows the attacker to execute arbitrary code. Failed exploits can cause denial of service.

SOLUTION:

Users are advised to upgrade to latest version of VLC which resolves these issues.Latest version can be obtained here (http://www.videolan.org/vlc/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Security Advisory 1302: Windows (http://www.videolan.org/vlc/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2013-3245
Description: ** DISPUTED ** plugins/demux/libmkv_plugin.dll in VideoLAN VLC Media Player 2.0.7, and possibly other versions, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted MKV file, possibly involving an integer overflow and out-of-bounds read or heap-based buffer overflow, or an uncaught exception. NOTE: the vendor disputes the severity and claimed vulnerability type of this issue, stating "This PoC crashes VLC, indeed, but does nothing more..
Link: http://seclists.org/fulldisclosure/2013/Jul/71

Reference: CVE-2013-1954
Description: The ASF Demuxer (modules/demux/asf/asf.c) in VideoLAN VLC media player 2.0.5 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted ASF movie that triggers an out-of-bounds read.
Link: http://git.videolan.org/?p=vlc.git;a=commitdiff;h=b31ce523331aa3a6e620b68cdfe3f161d519631e

Reference: CVE-2013-1954
Description: The ASF Demuxer (modules/demux/asf/asf.c) in VideoLAN VLC media player 2.0.5 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted ASF movie that triggers an out-of-bounds read.
Link: http://trac.videolan.org/vlc/ticket/8024

nist-nvd2

Reference: CVE-2013-3245
Description: plugins/demux/libmkv_plugin.dll in VideoLAN VLC Media Player 2.0.7, and possibly other versions, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted MKV file, possibly involving an integer overflow and out-of-bounds read or heap-based buffer overflow, or an uncaught exception. NOTE: the vendor disputes the severity and claimed vulnerability type of this issue, stating "This PoC crashes VLC, indeed, but does nothing more... this is not a
Link: http://seclists.org/fulldisclosure/2013/Jul/71

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 3 VLC Media Player Multiple Vulnerabilities

| | |
|---|---|
| QID: | 121380 |
| Category: | Local |
| Associated CVEs: | CVE-2013-4233, CVE-2013-4234, CVE-2013-4388, CVE-2013-6283 |
| Vendor Reference: | VLC Change Log |
| Bugtraq ID: | 61714,62724 |
| Service Modified: | 05/29/2023 |
| 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.
Multiple vulnerabilities have been reported in VLC media player which can be exploited by attacker to compromise a user's system or cause a denial of service:
-Two vulnerabilities are caused due to a bundled vulnerable version of libmodplug.
-An out-of-bounds write error within the "LOASParse()" function (modules/packetizer/mpeg4audio.c) can be exploited to cause a heap-based buffer overflow.
- A denial of service and possible arbitrary code execution vulnerability via a long string in a URL in a m3u file.
Affected Versions:
The vulnerability is confirmed in version 2.0.8. Older versions up-to 2.0.0 are also vulnerable.

IMPACT:

Successful exploitation of this vulnerability can cause an overflow that allows the attacker to execute arbitrary code. Failed exploits can cause denial of service.

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 2.1.0 (http://www.videolan.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2013-6283
Description: VideoLAN VLC Media Player 2.0.8 - '.m3u' Local Crash (PoC) - The Exploit-DB Ref : 27700
Link: http://www.exploit-db.com/exploits/27700

exploitdb

Reference: CVE-2013-6283
Description: VideoLAN VLC Media Player 2.0.8 - '.m3u' Local Crash (PoC)
Link: https://www.exploit-db.com/exploits/27700

nvd

Reference: CVE-2013-4388
Description: Buffer overflow in the mp4a packetizer (modules/packetizer/mpeg4audio.c) in VideoLAN VLC Media Player before 2.0.8 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.
Link: http://git.videolan.org/?p=vlc.git;a=commitdiff;h=9794ec1cd268c04c8bca13a5fae15df6594dff3e

Reference: CVE-2013-4233
Description: Integer overflow in the abc_set_parts function in load_abc.cpp in libmodplug 0.8.8.4 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted P header in an ABC file, which triggers a heap-based buffer overflow.
Link: http://www.openwall.com/lists/oss-security/2013/08/10/3

Reference: CVE-2013-4233
Description: Integer overflow in the abc_set_parts function in load_abc.cpp in libmodplug 0.8.8.4 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted P header in an ABC file, which triggers a heap-based buffer overflow.
Link: http://blog.scrt.ch/2013/07/24/vlc-abc-parsing-seems-to-be-a-ctf-challenge/

Reference: CVE-2013-4234
Description: Multiple heap-based buffer overflows in the (1) abc_MIDI_drum and (2) abc_MIDI_gchord functions in load_abc.cpp in libmodplug 0.8.8.4 and earlier allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via a crafted ABC.
Link: http://www.openwall.com/lists/oss-security/2013/08/10/3

Reference: CVE-2013-4234
Description: Multiple heap-based buffer overflows in the (1) abc_MIDI_drum and (2) abc_MIDI_gchord functions in load_abc.cpp in libmodplug 0.8.8.4 and earlier allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via a crafted ABC.
Link: http://blog.scrt.ch/2013/07/24/vlc-abc-parsing-seems-to-be-a-ctf-challenge/

Reference: CVE-2013-6283
Description: VideoLAN VLC Media Player 2.0.8 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string in a URL in a m3u file.
Link: http://www.exploit-db.com/exploits/27700

seebug

Reference: CVE-2013-6283

Description: VLC Player 2.0.8 (.m3u) - Local Crash PoC
Link: https://www.seebug.org/vuldb/ssvid-81297

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 3 VLC Media Player RTSP Processing "parseRTSPRequestString()" Buffer Overflow Vulnerability

| | |
|---|---|
| QID: | 121764 |
| Category: | Local |
| Associated CVEs: | CVE-2013-6934 |
| Vendor Reference: | - |
| Bugtraq ID: | 65139 |
| Service Modified: | 05/29/2023 |
| 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.
A buffer overflow vulnerability exist in the application due to the way it handles RTSP protocol data that is directly passed to parseRTSPRequestString(), which accepts user input without validation, which can be exploited to cause a buffer overflow.
Affected Versions:
VLC 2.1.1 and prior upto VLC 2.0.0

IMPACT:

Successful exploitation of this vulnerability can cause an overflow that allows the attacker to execute arbitrary code. Failed exploits can cause denial of service.

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:

Core Security
Reference: CVE-2013-6934
Description: VLC Media Player RTSP Processing Buffer Overflow Exploit - Core Security Category : Exploits/Client Side

nvd
Reference: CVE-2013-6934
Description: The parseRTSPRequestString function in Live Networks Live555 Streaming Media 2013.11.26, as used in VideoLAN VLC Media Player, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a space character at the beginning of an RTSP message, which triggers an integer underflow, infinite loop, and buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-6933.
Link: http://isecpartners.github.io/fuzzing/vulnerabilities/2013/12/30/vlc-vulnerability.html

coreimpact
Reference: CVE-2013-6934
Description: VLC Media Player RTSP Processing Buffer Overflow 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  Version is  2.0.0.0

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: | 03/26/2014 |
| 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  2.0.0.0

3 VLC Media Player Memory Corruption Vulnerability

| | |
|---|---|
| QID: | 122073 |
| Category: | Local |
| Associated CVEs: | CVE-2014-3441 |
| Vendor Reference: | - |
| Bugtraq ID: | 67315 |
| Service Modified: | 05/29/2023 |
| 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.

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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 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: | 05/29/2023 |
| 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.
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/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 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: | 05/29/2023 |
| 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 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 2.0.0.0

## 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: | 05/29/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 3 Mozilla Firefox SSL 3.0 Information Disclosure Vulnerability (POODLE)

| | |
|---|---|
| QID: | 122751 |
| Category: | Local |
| Associated CVEs: | CVE-2014-3566 |
| Vendor Reference: | POODLE |

| | |
|---|---|
| Bugtraq ID: | 70574 |
| Service Modified: | 08/15/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

The SSL protocol 3.0 design error, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attacks.
The Firefox browser on the target system supports SSLv3, which makes it vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption), even if it also supports more recent versions of TLS. The target is subject to a downgrade attack, in which the attacker tricks the browser into connecting with SSLv3.

IMPACT:

An attacker who can take a man-in-the-middle (MitM) position can exploit this vulnerability and gain access to encrypted communication between a client and server.

SOLUTION:

Disable SSLv3 support in your browser to avoid this vulnerability.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2014-3566
Description: HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/ssl_version
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

Reference: CVE-2014-3566
Description: HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/axis_local_file_include
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

Reference: CVE-2014-3566
Description: HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/spoof/cisco/dtp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

seebug

Reference: CVE-2014-3566
Description: SSL 3.0 POODLE（CVE-2014-3566）
Link: https://www.seebug.org/vuldb/ssvid-92692

metasploit

Reference: CVE-2014-3566
Description: SSL/TLS Version Detection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/ssl/ssl_version.rb

cisa-alerts

Reference: CVE-2014-3566
Description: SSL 3.0 Protocol Vulnerability and POODLE Attack
Link: https://cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack

Reference: CVE-2014-3566
Description: SSL 3.0 Protocol Vulnerability and POODLE Attack
Link: https://www.cisa.gov/ncas/alerts/TA14-290A

Reference: CVE-2014-3566
Description: SSL 3.0 Protocol Vulnerability and POODLE Attack
Link: https://www.us-cert.gov/ncas/alerts/TA14-290A

github-exploits

Reference: CVE-2014-3566
Description: mpgn/poodle-PoC exploit repository

Link: https://github.com/mpgn/poodle-PoC

coreimpact

Reference: CVE-2014-3566
Description: POODLE TLS1.x to SSLv3 Downgrading Vulnerability Exploit
Link: https://www.coresecurity.com/core-labs/exploits

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0
The following user account paths are detected:
%systemdrive%\users\vboxuser\AppData\Roaming\Mozilla\Firefox\Profiles\default.knd\prefs.js

### 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 2.0.0.0

### 3 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-43 and MFSA 2015-44)

| | |
|---|---|
| QID: | 123510 |
| Category: | Local |
| Associated CVEs: | CVE-2015-0798, CVE-2015-0799 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-43 and MFSA 2015-44 |
| Bugtraq ID: | - |
| Service Modified: | 04/13/2015 |
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities.
Affected Versions:
Mozilla Firefox versions prior to 37.0.1

IMPACT:

A remote attacker can exploit this vulnerability to obtain potentially sensitive information or conduct a man-in-the-middle attack that can bypass certificate verification.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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 1.7.0.0

### 3 Mozilla Firefox Plugin Initialization Memory Corruption Vulnerability

| | |
|---|---|
| QID: | 123571 |
| Category: | Local |
| Associated CVEs: | CVE-2015-2706 |
| Vendor Reference: | MFSA 2015-45 |
| Bugtraq ID: | 74247 |
| Service Modified: | 05/06/2015 |
| 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.
Firefox has been reported vulnerable to use-after-free vulnerability which exist due to a race condition when initialization of a plugins, which can be exploited by an attacker to execute arbitrary code
Affected Versions:
Mozilla Firefox versions prior to 37.0.2

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 released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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 1.7.0.0

### 3 Mozilla Firefox Same Origin Violation And Local File Stealing Vulnerability (MFSA 2015-78)

| | |
|---|---|
| QID: | 123791 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4495 |
| Vendor Reference: | Mozilla Advisory MFSA 2015-78 |
| Bugtraq ID: | 76249 |
| Service Modified: | 08/15/2023 |
| 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.
A flaw was discovered in Mozilla Firefox that could be used to violate the same-origin policy and inject web script into a non-privileged part of the built-in PDF file viewer (PDF.js). An attacker could exploit this vulnerability by persuading a user to visit a malicious web page. Once viewed, it could read and steal arbitrary files from the system running Firefox.
Affected Versions:
Mozilla Firefox versions prior to 39.0.3
Mozilla Firefox ESR versions prior to 38.1.1
Note: Mozilla has received reports that an exploit based on this vulnerability has been found in the wild.

IMPACT:

Successful exploitation of this vulnerability could allow an attacker to read and steal sensitive local files on the victim's computer.

SOLUTION:

The vendor has released an advisory and update to fix this vulnerability. Refer to MFSA2015-78 (https://www.mozilla.org/en-US/security/advisories/mfsa2015-78/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
Metasploit

Reference: CVE-2015-4495
Description: Firefox PDF.js Browser File Theft - Metasploit Ref : /modules/auxiliary/gather/firefox_pdfjs_file_theft
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/gather/firefox_pdfjs_file_theft.rb

Reference: CVE-2015-4495
Description: Firefox PDF.js Browser File Theft - Metasploit Ref : /modules/exploit/multi/browser/firefox_queryinterface
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/gather/firefox_pdfjs_file_theft.rb

The Exploit-DB
Reference: CVE-2015-4495
Description: Mozilla Firefox < 39.03 - 'pdf.js' Same Origin Policy - The Exploit-DB Ref : 37772
Link: http://www.exploit-db.com/exploits/37772

exploitdb
Reference: CVE-2015-4495
Description: Mozilla Firefox < 39.03 - 'pdf.js' Same Origin Policy
Link: https://www.exploit-db.com/exploits/37772

seebug
Reference: CVE-2015-4495
Description: Firefox < 39.0.3 - pdf.js Same Origin Policy Exploit
Link: https://www.seebug.org/vuldb/ssvid-89280

packetstorm
Reference: CVE-2015-4495
Description: Firefox Same Origin Policy Bypass
Link: https://packetstormsecurity.com/files/133113/Firefox-Same-Origin-Policy-Bypass.html

canvas
Reference: CVE-2015-4495
Description: firefox_pdfjs_filereader
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/firefox_pdfjs_filereader

metasploit
Reference: CVE-2015-4495
Description: Firefox PDF.js Browser File Theft
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/gather/firefox_pdfjs_file_theft.rb

0day.today
Reference: CVE-2015-4495
Description: Firefox 39.03 - pdf.js Same Origin Policy Exploit
Link: https://0day.today/exploit/24048

cisa-kev
Reference: CVE-2015-4495
Description: Mozilla Firefox Security Feature Bypass Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw
Reference: CVE-2015-4495
Description: Mozilla Firefox Same-origin policy bypass in PDF reader
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: MetaSploit
Type: Hacktool
Platform: Script

Malware ID: Heuristic

| | |
|---|---|
| Type: | Trojan |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | CVE-2015-4495 |
| Type: | Exploit |
| Platform: | Script |

| | |
|---|---|
| Malware ID: | Evisnefo |
| Type: | Exploit |
| Platform: | Win32 |

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

 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 2.0.0.0

 3 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-13 to MFSA 2016-14)

| | |
|---|---|
| QID: | 124696 |
| Category: | Local |
| Associated CVEs: | CVE-2016-1523, CVE-2016-1949 |
| Vendor Reference: | Mozilla Advisory MFSA 2016-13 to MFSA 2016-14 |
| Bugtraq ID: | 82991 |
| Service Modified: | 02/17/2016 |

| | |
|---|---|
| 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.
The Mozilla Foundation has released updates to address multiple vulnerabilities in Firefox.
Affected Versions:
Mozilla Firefox versions prior to 44.0.2
Mozilla Firefox ESR versions prior to 38.6.1

IMPACT:

Successful exploitation of these vulnerabilities will allow an attacker to execute arbitrary code or bypass the Same-origin policy, failed exploits may result in denial of service

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories (http://www.mozilla.org/security/announce/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (http://www.mozilla.org/en-US/firefox/new/)

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  1.7.0.0

### 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 2.0.0.0

### 3 Mozilla Firefox Arbitrary code execution vulnerability (MFSA2018-05)

| | |
|---|---|
| QID: | 370747 |
| Category: | Local |
| Associated CVEs: | CVE-2018-5124 |
| Vendor Reference: | MFSA2018-05 |
| Bugtraq ID: | - |
| Service Modified: | 06/18/2020 |
| 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.
Unsanitized output in the browser UI can lead to arbitrary code execution in Mozilla firefox prior to 58.0.1
Affected Versions:
Firefox prior to 58.0.1

IMPACT:

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code .

SOLUTION:

Refer to mfsa2018-05 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-05: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/)
mfsa2018-05: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/)

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  1.7.0.0

### 3 Mozilla Firefox Heap Buffer Overflow Vulnerability (MFSA2018-14)

| | |
|---|---|
| QID: | 370991 |
| Category: | Local |
| Associated CVEs: | CVE-2018-6126 |
| Vendor Reference: | MFSA2018-14 |
| Bugtraq ID: | 104309,104411 |
| Service Modified: | 05/30/2023 |
| 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.

Firefox is vulnerable to Heap-Buffer-Overflow vulnerability.A heap buffer overflow can occur in the Skia library when rasterizing paths using a maliciously crafted SVG file with anti-aliasing turned off. This results in a potentially exploitable crash.
Affected Versions:
Firefox prior to 60.0.2
Firefox ESR prior to 52.8.1
Firefox ESR prior to 60.0.2

IMPACT:

On successful exploitation this vulnerability can potentially be used by an attacker to crash the system.

SOLUTION:

Refer to mfsa2018-14  (https://www.mozilla.org/en-US/security/advisories/mfsa2018-14/) .
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-14 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-14/)
mfsa2018-14 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-14/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
- Reference: CVE-2018-6126
- Description: Skia - Heap Overflow in SkScan::FillPath due to Precision Error - The Exploit-DB Ref : 45098
- Link: http://www.exploit-db.com/exploits/45098

exploitdb
- Reference: CVE-2018-6126
- Description: Skia - Heap Overflow in SkScan::FillPath due to Precision Error
- Link: https://www.exploit-db.com/exploits/45098

nvd
- Reference: CVE-2018-6126
- Description: A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.

Link: https://crbug.com/844457

packetstorm
Reference: CVE-2018-6126
Description: Skia SkScan::FillPath Heap Overflow
Link: https://packetstormsecurity.com/files/148684/Skia-SkScan-FillPath-Heap-Overflow.html

0day.today
Reference: CVE-2018-6126
Description: Skia - Heap Overflow in SkScan::FillPath due to Precision Error Vulnerability
Link: https://0day.today/exploit/30792

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2018-15, MFSA2018-16, MFSA2018-17)

| | |
|---|---|
| QID: | 371026 |
| Category: | Local |
| Associated CVEs: | CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-12358, CVE-2018-12362, CVE-2018-5156, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365, CVE-2018-12371, CVE-2018-12366, CVE-2018-12367, CVE-2018-12368, CVE-2018-12369, CVE-2018-12370, CVE-2018-5186, CVE-2018-5187, CVE-2018-5188 |
| Vendor Reference: | MFSA2018-15, MFSA2018-16, MFSA2018-17 |
| Bugtraq ID: | 104246,104561,104560,104555,104558,104557,104556 |
| Service Modified: | 05/30/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.
Firefox is found to be vulnerable to the following:
CVE-2018-12359 - Buffer overflow using computed size of canvas element
CVE-2018-12360 - Use-after-free when using focus()
CVE-2018-12361 - Integer overflow in SwizzleData
CVE-2018-12358 - Same-origin bypass using service worker and redirection
CVE-2018-12362 - Integer overflow in SSSE3 scaler
CVE-2018-5156 - Media recorder segmentation fault when track type is changed during capture
CVE-2018-12363 - Use-after-free when appending DOM nodes
CVE-2018-12364 - CSRF attacks through 307 redirects and NPAPI plugins
CVE-2018-12365 - Compromised IPC child process can list local filenames
CVE-2018-12371 - Integer overflow in Skia library during edge builder allocation
CVE-2018-12366 - Invalid data handling during QCMS transformations
CVE-2018-12367 - Timing attack mitigation of PerformanceNavigationTiming
CVE-2018-12368 - No warning when opening executable SettingContent-ms files
CVE-2018-12369 - WebExtension security permission checks bypassed by embedded experiments
CVE-2018-12370 - SameSite cookie protections bypassed when exiting Reader View
CVE-2018-5186 - Memory safety bugs fixed in Firefox 61
CVE-2018-5187 - Memory safety bugs fixed in Firefox 60 and Firefox ESR 60.1
CVE-2018-5188 - Memory safety bugs fixed in Firefox 60, Firefox ESR 60.1, and Firefox ESR 52.9
Affected Versions:
versions prior to Firefox 61
versions prior to Firefox ESR 60.1
versions prior to Firefox ESR 52.9

IMPACT:

On successful exploitation this vulnerability can potentially be used by an attacker to perform CSRF attacks, expose private local files, leak information, execute arbitrary code and crash the system.

SOLUTION:

The vendor has released patch which can be found here (https://www.mozilla.org/en-US/firefox/new/) and here (https://www.mozilla.org/en-US/firefox/organizations/).

Please refer to mfsa2018-15 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-15/), mfsa2018-16 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-16/), mfsa2018-17 (https://www.mozilla.org/en-US/security/advisories/mfsa2018-17/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2018-15: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-15/)
mfsa2018-15: Mac OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-15/)
mfsa2018-16: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-16/)
mfsa2018-16: Mac OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-16/)
mfsa2018-17: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-17/)
mfsa2018-17: Mac OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-17/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2018-12368
Description: Windows 10 does not warn users before opening executable files with the SettingContent-ms extension even when they have been downloaded from the internet and have the "Mark of the Web." Without the warning, unsuspecting users unfamiliar with this new file type might run an unwanted executable. This also allows a WebExtension with the limited downloads.open permission to execute arbitrary code without user interaction on Windows 10 systems. *Note: this issue only affects Windows operating systems
Link: https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39

Reference: CVE-2018-12371
Description: An integer overflow vulnerability in the Skia library when allocating memory for edge builders on some systems with at least 16 GB of RAM. This results in the use of uninitialized memory, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.1, Thunderbird < 60, and Firefox < 61.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1465686

Reference: CVE-2018-5186
Description: Memory safety bugs present in Firefox 60. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 61.
Link: https://bugzilla.mozilla.org/buglist.cgi?bug_id=1464872%2C1463329%2C1419373%2C1412882%2C1413033%2C1444673%2C1454448%2C1453505%

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 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: | 08/15/2023 |
| 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.
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

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2018-11529
Type: Exploit
Platform: Win32

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

3 Mozilla Firefox Multiple Vulnerabilities(MFSA 2019-09,MFSA2019-10)

| | |
|---|---|
| QID: | 371702 |
| Category: | Local |
| Associated CVEs: | CVE-2019-9810, CVE-2019-9813 |
| Vendor Reference: | MFSA 2019-09, MFSA 2019-10 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| 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 and Firefox ESR is prone to following vulnerabilities:
CVE-2019-9810: Incorrect alias information in IonMonkey MArraySlice.
CVE-2019-9813: Ionmonkey type confusion with __proto__ mutations.
Affected Versions:
Prior to Firefox 66.0.1
Prior to Firefox ESR 60.6.1

IMPACT:

Successful exploitation of this vulnerability could lead to arbitrary memory read and write.

SOLUTION:

The Vendor has released fixes to address these vulnerabilities. Please refer to MFSA2019-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-09/)
And MFSA2019-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-09: Windows, Mac (https://www.mozilla.org/en-US/security/advisories/mfsa2019-09/)
MFSA2019-10: Windows, Mac (https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2019-9813

Description: SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion) - The Exploit-DB Ref : 46646
Link: http://www.exploit-db.com/exploits/46646

Reference: CVE-2019-9810
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack - The Exploit-DB Ref : 47752
Link: http://www.exploit-db.com/exploits/47752

Reference: CVE-2019-9810
Description: Firefox < 66.0.1 - 'Array.prototype.slice' Buffer Overflow - The Exploit-DB Ref : 46605
Link: http://www.exploit-db.com/exploits/46605

exploitdb

Reference: CVE-2019-9810
Description: Firefox < 66.0.1 - 'Array.prototype.slice' Buffer Overflow
Link: https://www.exploit-db.com/exploits/46605

Reference: CVE-2019-9810
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack
Link: https://www.exploit-db.com/exploits/47752

Reference: CVE-2019-9813
Description: SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion)
Link: https://www.exploit-db.com/exploits/46646

nvd

Reference: CVE-2019-9810
Description: Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1537924

Reference: CVE-2019-9810
Description: Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.
Link: http://packetstormsecurity.com/files/155592/Mozilla-Firefox-Windows-64-Bit-Chain-Exploit.html

packetstorm

Reference: CVE-2019-9810
Description: Mozilla Firefox Windows 64-Bit Chain Exploit
Link: https://packetstormsecurity.com/files/155592/Mozilla-Firefox-Windows-64-Bit-Chain-Exploit.html

Reference: CVE-2019-9810
Description: Firefox Array.prototype.slice Buffer Overflow
Link: https://packetstormsecurity.com/files/152251/Firefox-Array.prototype.slice-Buffer-Overflow.html

Reference: CVE-2019-9813
Description: SpiderMonkey IonMonkey Type Confusion
Link: https://packetstormsecurity.com/files/152304/SpiderMonkey-IonMonkey-Type-Confusion.html

0day.today

Reference: CVE-2019-9810
Description: Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack Exploit
Link: https://0day.today/exploit/33639

Reference: CVE-2019-9810
Description: Firefox 66.0.1 - Array.prototype.slice Buffer Overflow Exploit
Link: https://0day.today/exploit/32423

Reference: CVE-2019-9813
Description: SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion)
Link: https://0day.today/exploit/32482

github-exploits

Reference: CVE-2019-9810
Description: 0vercl0k/CVE-2019-11708 exploit repository
Link: https://github.com/0vercl0k/CVE-2019-11708

Reference: CVE-2019-9810
Description: 0vercl0k/CVE-2019-9810 exploit repository
Link: https://github.com/0vercl0k/CVE-2019-9810

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2019-9810
Type: Exploit
Platform: Win32,Script,Win64

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

3 Mozilla Firefox Multiple Security Vulnerabilities (MFSA 2019-13,MFSA 2019-14)

| | |
|---|---|
| QID: | 371797 |
| Category: | Local |
| Associated CVEs: | CVE-2018-18511, CVE-2019-11691, CVE-2019-11692, CVE-2019-11693, CVE-2019-11694, CVE-2019-11695, CVE-2019-11696, CVE-2019-11697, CVE-2019-11698, CVE-2019-11699, CVE-2019-11700, CVE-2019-11701, CVE-2019-5798, CVE-2019-7317, CVE-2019-9797, CVE-2019-9800, CVE-2019-9814, CVE-2019-9815, CVE-2019-9816, CVE-2019-9817, CVE-2019-9818, CVE-2019-9819, CVE-2019-9820, CVE-2019-9821 |
| Vendor Reference: | MFSA2019-13, MFSA2019-14 |
| Bugtraq ID: | 108098 |
| Service Modified: | 05/31/2023 |
| 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.
Multiple security vulnerabilities were found in Mozilla Firefox.
Affected Versions:
Prior to Firefox 67
Prior to Firefox ESR 60.7

IMPACT:

Successful exploitation affects confidentiality, integrity and availability of the product and the system.

SOLUTION:

The vendor has released Firefox ESR 60.7 and Firefox 67 to fix this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (https://www.mozilla.org/en-US/firefox/new/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2019-9816
Description: Spidermonkey - IonMonkey Unexpected ObjectGroup in ObjectGroupDispatch Operation - The Exploit-DB Ref : 46940
Link: http://www.exploit-db.com/exploits/46940

exploitdb
Reference: CVE-2019-9816

Description: Spidermonkey - IonMonkey Unexpected ObjectGroup in ObjectGroupDispatch Operation
Link: https://www.exploit-db.com/exploits/46940

nvd

Reference: CVE-2019-7317
Description: png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
Link: https://github.com/glennrp/libpng/issues/275

Reference: CVE-2019-11695
Description: A custom cursor defined by scripting on a site can position itself over the addressbar to spoof the actual cursor when it should not be allowed outside of the primary web content area. This could be used by a malicious site to trick users into clicking on permission prompts, doorhanger notifications, or other buttons inadvertently if the location is spoofed over the user interface. This vulnerability affects Firefox < 67.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1445844

Reference: CVE-2019-11696
Description: Files with the .JNLP extension used for "Java web start" applications are not treated as executable content for download prompts even though they can be executed if Java is installed on the local system. This could allow users to mistakenly launch an executable binary locally. This vulnerability affects Firefox < 67.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1392955

Reference: CVE-2019-5798
Description: Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
Link: https://crbug.com/883596

0day.today

Reference: CVE-2019-9816
Description: Spidermonkey - IonMonkey Unexpected ObjectGroup in ObjectGroupDispatch Operation Exploit
Link: https://0day.today/exploit/32815

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 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: | 05/31/2023 |
| 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 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 3 Mozilla Firefox Unauthorised Local File Access Vulnerability (MFSA2019-16)

| | |
|---|---|
| QID: | 371841 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11702 |
| Vendor Reference: | MFSA2019-16 |
| Bugtraq ID: | - |
| Service Modified: | 06/16/2020 |
| 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.
A hyperlink using protocols associated with Internet Explorer, such as IE.HTTP, can be used to open local files at a known location with Internet Explorer if a user approves execution when prompted.
Affected Version:
Prior to Firefox 67.0.2

IMPACT:

Successful exploitation of this vulnerability can be used to open local files at a known location with Internet Explorer.

SOLUTION:

The vendor has released Firefox 67.0.2 to fix this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Mozilla Firefox (https://www.mozilla.org/en-US/security/advisories/mfsa2019-16/)

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 1.7.0.0

## 3 Mozilla Firefox and Firefox ESR Multiple Vulnerabilities (MFSA2019-21)(MFSA2019-22)

| | |
|---|---|
| QID: | 372001 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11709, CVE-2019-11710, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11714, CVE-2019-11715, CVE-2019-11716, CVE-2019-11717, CVE-2019-11718, CVE-2019-11719, CVE-2019-11720, CVE-2019-11721, CVE-2019-11723, CVE-2019-11724, CVE-2019-11725, CVE-2019-11727, CVE-2019-11728, CVE-2019-11729, CVE-2019-11730, CVE-2019-9811 |
| Vendor Reference: | MFSA 2019-21, ,MFSA 2019-22 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefoxis a free and open source web browser which is made by the Mozilla Foundation and its subsidiary, the Mozilla Corporation. It works on common operating systems, such as Windows, macOS, Linux and Android.

Affected Products:
Prior to Firefox 68 and Firefox ESR 60.8

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-22 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/)
Refer to MFSA2019-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2019-22 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/)
MFSA 2019-21 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2019-11721
Description: The unicode latin 'kra' character can be used to spoof a standard 'k' character in the addressbar. This allows for domain spoofing attacks as do not display as punycode text, allowing for user confusion. This vulnerability affects Firefox < 68.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1256009

Reference: CVE-2019-11724
Description: Application permissions give additional remote troubleshooting permission to the site input.mozilla.org, which has been retired and now redirects to another site. This additional permission is unnecessary and is a potential vector for malicious attacks. This vulnerability affects Firefox < 68.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1512511

Reference: CVE-2019-11717
Description: A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1548306

Reference: CVE-2019-9811
Description: As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1539598

Reference: CVE-2019-9811
Description: As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1563327

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 3 Mozilla Firefox and Firefox ESR Vulnerability (MFSA 2019-24)

| | |
|---|---|
| QID: | 372061 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11733 |
| Vendor Reference: | MFSA 2019-24 |
| Bugtraq ID: | - |
| Service Modified: | 06/13/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefoxis a free and open source web browser which is made by the Mozilla Foundation and its subsidiary, the Mozilla Corporation. It works on common operating systems, such as Windows, macOS, Linux and Android.

Affected Products:
Prior to Firefox 68.0.2 and Firefox ESR 68.0.2

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-24/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2019-24 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-24/)

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 1.7.0.0

### 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: | 05/30/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

## 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2019-31)

| | |
|---|---|
| QID: | 372136 |
| Category: | Local |
| Associated CVEs: | CVE-2019-11754 |
| Vendor Reference: | MFSA2019-31 |
| Bugtraq ID: | - |
| Service Modified: | 11/25/2020 |
| 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.
CVE-2019-11754: Pointer Lock is enabled with no user notification
Affected Products: Prior to Firefox 69.0.1

IMPACT:

On successful exploitation it could allow an attacker to execute code.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2019-31 (https://www.mozilla.org/en-US/security/advisories/mfsa2019-31)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2019-31: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2019-31)
MFSA2019-31: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2019-31)

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 1.7.0.0

### 3 VideoLAN VLC Media player Denial of Service Vulnerability

| | |
|---|---|
| QID: | 372568 |
| Category: | Local |
| Associated CVEs: | CVE-2012-3377 |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 05/29/2023 |
| 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 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:

nvd

Reference: CVE-2012-3377
Description: 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.
Link: http://git.videolan.org/?p=vlc/vlc-2.0.git;a=commitdiff;h=16e9e126333fb7acb47d363366fee3deadc8331e

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\VideoLAN\VLC\vlc.exe Version is 2.0.0.0

### 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 2.0.0.0

### 3 Mozilla Firefox Cross-Origin Policy Vulnerabiltiy

| | |
|---|---|
| QID: | 372649 |
| Category: | Local |
| Associated CVEs: | CVE-2015-7184 |
| Vendor Reference: | mfsa2015-115 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2020 |
| 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.
Firefox Prior to 41.0.2 has same origin policy violation vulnerability.
Affected Versions:
Prior to 41.0.2

IMPACT:

Succssful exploitation could allow user to violate same origin policy against a domain if it loads resources from malicious sites.

SOLUTION:

The vendor has released advisories and updates to fix these vulnerabilities. Refer to Mozilla Security Advisories

(https://www.mozilla.org/en-US/security/advisories/mfsa2015-115/) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2015-115 (https://www.mozilla.org/en-US/security/advisories/mfsa2015-115/)

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  1.7.0.0

3 Mozilla Firefox Security Update(MFSA2020-28)

| | |
|---|---|
| QID: | 373120 |
| Category: | Local |
| Associated CVEs: | CVE-2020-15648 |
| Vendor Reference: | MFSA2020-28 |
| Bugtraq ID: | - |
| Service Modified: | 08/13/2020 |
| 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 by Following vulnerabilities:
CVE-2020-15648: X-Frame-Options bypass using object or embed tags.
Affected Products :
Prior to Firefox 78.0.2

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2020-28 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-28/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2020-28 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-28/)

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  1.7.0.0

3 Mozilla Firefox Multiple Vulnerabilities (MFSA2020-31)

| | |
|---|---|
| QID: | 373326 |
| Category: | Local |

| | |
|---|---|
| Associated CVEs: | CVE-2020-15652, CVE-2020-6514, CVE-2020-6463, CVE-2020-15650, CVE-2020-15649, CVE-2020-15659 |
| Vendor Reference: | MFSA2020-31 |
| Bugtraq ID: | - |
| Service Modified: | 05/31/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a free and open-source web browser developed for Windows, OS X, and Linux, with a mobile version for Android.
Firefox is found to be vulnerable to the following:
CVE-2020-15652: Potential leak of redirect targets when loading scripts in a worker
CVE-2020-6514: WebRTC data channel leaks internal address to peer
CVE-2020-6463: Use-after-free in ANGLE gl::Texture::onUnbindAsSamplerTexture
CVE-2020-15650:Overwriting local files through malicious file picker application
CVE-2020-15649: Exfiltrating local files through malicious file picker application
CVE-2020-15659:Memory safety bugs fixed in Firefox 79 and Firefox ESR 68.11

Affected Versions:
versions prior to Firefox ESR 68.11

IMPACT:

On successful exploitation attacker could compromise confidentiality, integrity and availability of the software.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to
mfsa2020-31 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2020-31 (https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2020-6514
Description: Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.
Link: https://crbug.com/1076703

Reference: CVE-2020-6514
Description: Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.
Link: http://packetstormsecurity.com/files/158697/WebRTC-usrsctp-Incorrect-Call.html

0day.today

Reference: CVE-2020-6514
Description: WebRTC usrsctp Incorrect Call Vulnerability
Link: https://0day.today/exploit/34769

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 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: | 05/31/2023 |
| 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 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/CVE-2020-26

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 2.0.0.0

## 3 Mozilla Firefox Out of Bound Read Vulnerability (MFSA2021-27)

| | |
|---|---|
| QID: | 375642 |
| Category: | Local |
| Associated CVEs: | CVE-2021-29968 |
| Vendor Reference: | MFSA2021-27 |
| Bugtraq ID: | - |
| Service Modified: | 07/02/2021 |
| 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.
CVE-2021-29968: When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur.
Affected Products:
Prior to Firefox 89.0.1
NOTE:
This bug only affects Firefox on Windows. Other operating systems are unaffected.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to read sensitive file.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA 2021-27 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-27/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-27 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-27/)

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  1.7.0.0

## 3 Mozilla Firefox Header Splitting Vulnerability(MFSA2021-37)

| | |
|---|---|
| QID: | 375824 |
| Category: | Local |
| Associated CVEs: | CVE-2021-29991 |
| Vendor Reference: | MFSA2021-37 |
| Bugtraq ID: | - |
| Service Modified: | 11/05/2021 |
| 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 91

IMPACT:

This allowed for a header splitting attack against servers using HTTP/3.

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-37 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-37 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/)

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  1.7.0.0

3 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-43)

| | |
|---|---|
| QID: | 375945 |
| Category: | Local |
| Associated CVEs: | CVE-2021-38496, CVE-2021-38497, CVE-2021-38498, CVE-2021-38499, CVE-2021-32810, CVE-2021-38500, CVE-2021-38501 |
| Vendor Reference: | MFSA2021-43 |
| Bugtraq ID: | - |
| Service Modified: | 10/08/2021 |
| 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 93

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity, and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-43 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-43/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-43 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-43/)

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  1.7.0.0

3 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-48)

| | |
|---|---|
| QID: | 376015 |
| Category: | Local |
| Associated CVEs: | CVE-2021-38503, CVE-2021-38504, CVE-2021-38505, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509, CVE-2021-38510 |
| Vendor Reference: | MFSA2021-48 |
| Bugtraq ID: | - |
| Service Modified: | 12/14/2021 |
| 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 94

IMPACT:

Successful exploitation of this vulnerability could compromise confidentiality, integrity, and availability

SOLUTION:

Vendor has released fix to address these vulnerabilities. Refer to MFSA2021-48 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-48)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-48 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-48)

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  1.7.0.0

 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2021-52)

| | |
|---|---|
| QID: | 376143 |
| Category: | Local |
| Associated CVEs: | CVE-2021-43543, CVE-2021-43546, CVE-2021-43541, CVE-2021-43540, CVE-2021-43536, CVE-2021-43544, CVE-2021-43545, CVE-2021-43537, CVE-2021-43539, CVE-2021-43538, CVE-2021-43542 |
| Vendor Reference: | MFSA2021-52 |
| Bugtraq ID: | - |
| Service Modified: | 12/11/2021 |
| 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-2021-43536: URL leakage when navigating while executing asynchronous function
CVE-2021-43537: Heap buffer overflow when using structured clone
CVE-2021-43538: Missing fullscreen and pointer lock notification when requesting both
CVE-2021-43539: GC rooting failure when calling wasm instance methods
CVE-2021-43540: WebExtensions could have installed persistent ServiceWorkers
CVE-2021-43541: External protocol handler parameters were unescaped
CVE-2021-43542: XMLHttpRequest error codes could have leaked the existence of an external protocol handler
CVE-2021-43543: Bypass of CSP sandbox directive when embedding
CVE-2021-43544: Receiving a malicious URL as text through a SEND intent could have led to XSS
CVE-2021-43545: Denial of Service when using the Location API in a loop
CVE-2021-43546: Cursor spoofing could overlay user interface when native cursor is zoomed
Affected Products:
Prior to Firefox 95

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 MFSA2021-52 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2021-52/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2021-52 (https://www.mozilla.org/en-US/security/advisories/mfsa2021-52/)

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  1.7.0.0

### 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-01)

| | |
|---|---|
| QID: | 376237 |
| Category: | Local |
| Associated CVEs: | CVE-2022-22741, CVE-2022-22746, CVE-2022-22742, CVE-2022-22747, CVE-2022-22736, CVE-2022-22751, CVE-2022-22748, CVE-2022-22740, CVE-2022-22749, CVE-2022-22744, CVE-2022-22739, CVE-2022-22750, CVE-2022-22745, CVE-2022-22752, CVE-2022-22743, CVE-2022-22737, CVE-2022-22738, CVE-2021-4140 |
| Vendor Reference: | MFSA2022-01 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-22746: Calling into reportValidity could have lead to fullscreen window spoof
CVE-2022-22743: Browser window spoof using fullscreen mode
CVE-2022-22742: Out-of-bounds memory access when inserting text in edit mode
CVE-2022-22741: Browser window spoof using fullscreen mode
CVE-2022-22740: Use-after-free of ChannelEventQueue::mOwner
CVE-2022-22738: Heap-buffer-overflow in blendGaussianBlur
CVE-2022-22737: Race condition when playing audio files
CVE-2021-4140: Iframe sandbox bypass with XSLT
CVE-2022-22750: IPC passing of resource handles could have lead to sandbox bypass
CVE-2022-22749: Lack of URL restrictions when scanning QR codes
CVE-2022-22748: Spoofed origin on external protocol launch dialog
CVE-2022-22745: Leaking cross-origin URLs through securitypolicyviolation event
CVE-2022-22744: The 'Copy as curl' feature in DevTools did not fully escape website-controlled data, potentially leading to command injection
CVE-2022-22747: Crash when handling empty pkcs7 sequence
CVE-2022-22736: Potential local privilege escalation when loading modules from the install directory.
CVE-2022-22739: Missing throttling on external protocol launch dialog
CVE-2022-22751: Memory safety bugs fixed in Firefox 96 and Firefox ESR 91.5
CVE-2022-22752: Memory safety bugs fixed in Firefox 96
Affected Products:
Prior to Firefox 96

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 MFSA2022-01 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-01 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2021-4140
Description: It was possible to construct specific XSLT markup that would be able to bypass an iframe sandbox. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1746720

Reference: CVE-2022-22737
Description: Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1745874

Reference: CVE-2022-22738
Description: Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1742382

Reference: CVE-2022-22739
Description: Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1744158

Reference: CVE-2022-22740
Description: Certain network request objects were freed too early when releasing a network request handle. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1742334

Reference: CVE-2022-22748
Description: Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1705211

Reference: CVE-2022-22736
Description: If Firefox was installed to a world-writable directory, a local privilege escalation could occur when Firefox searched the current directory for system libraries. However the install directory is not world-writable by default.*This bug only affects Firefox for Windows in a non-default installation. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1742692

Reference: CVE-2022-22749
Description: When scanning QR codes, Firefox for Android would have allowed navigation to some URLs that do not point to web content.*This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1705094

Reference: CVE-2022-22750
Description: By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to.*This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1566608

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0


3 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-04)

| | |
|---|---|
| QID: | 376387 |
| Category: | Local |
| Associated CVEs: | CVE-2022-22753, CVE-2022-22758, CVE-2022-22757, CVE-2022-22755, CVE-2022-22762, CVE-2022-0511, CVE-2022-22764, CVE-2022-22760, CVE-2022-22761, CVE-2022-22754, CVE-2022-22756, CVE-2022-22759 |
| Vendor Reference: | MFSA2022-04 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-22753: Privilege Escalation to SYSTEM on Windows via Maintenance Service
CVE-2022-22754: Extensions could have bypassed permission confirmation during update
CVE-2022-22755: XSL could have allowed JavaScript execution after a tab was closed
CVE-2022-22756: Drag and dropping an image could have resulted in the dropped object being an executable
CVE-2022-22757: Remote Agent did not prevent local websites from connecting
CVE-2022-22758: tel: links could have sent USSD codes to the dialer on Firefox for Android
CVE-2022-22759: Sandboxed iframes could have executed script if the parent appended elements
CVE-2022-22760: Cross-Origin responses could be distinguished between script and non-script content-types
CVE-2022-22761: frame-ancestors Content Security Policy directive was not enforced for framed extension pages
CVE-2022-22762: JavaScript Dialogs could have been displayed over other domains on Firefox for Android
CVE-2022-22764: Memory safety bugs fixed in Firefox 97 and Firefox ESR 91.6
CVE-2022-0511: Memory safety bugs fixed in Firefox 97
Affected Products:
Prior to Firefox 97

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 MFSA2022-04 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-04/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-04 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-04/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-22753
Description: A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access.*This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1732435

Reference: CVE-2022-22756
Description: If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1317873

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-09)

| | |
|---|---|
| QID: | 376447 |
| Category: | Local |
| Associated CVEs: | CVE-2022-26485, CVE-2022-26486 |
| Vendor Reference: | MFSA2022-09 |
| Bugtraq ID: | - |
| Service Modified: | 06/16/2023 |
| 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-2022-26485: Use-after-free in XSLT parameter processing
CVE-2022-26486: Use-after-free in WebGPU IPC Framework
Affected Products:
Prior to Firefox 97.0.2

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. Refer to MFSA2022-09 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-09 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-26485
Description: Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1758062

Reference: CVE-2022-26486
Description: An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1758070

Reference: CVE-2022-26486
Description: An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0.
Link: https://www.mozilla.org/security/advisories/mfsa2022-09/

cisa-alerts

Reference: CVE-2022-26485
Description: CISA Adds 11 Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2022/03/07/cisa-adds-11-known-exploited-vulnerabilities-catalog

Reference: CVE-2022-26486
Description: CISA Adds 11 Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2022/03/07/cisa-adds-11-known-exploited-vulnerabilities-catalog

github-exploits

Reference: CVE-2022-26485
Description: mistymntncop/CVE-2022-26485 exploit repository
Link: https://github.com/mistymntncop/CVE-2022-26485

cisa-kev

Reference: CVE-2022-26485
Description: Mozilla Firefox Use-After-Free Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2022-26486
Description: Mozilla Firefox Use-After-Free Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

google-0day-itw

Reference: CVE-2022-26485
Description: Mozilla Firefox Use-after-free inXSLT parameter processing
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2022-26486
Description: Mozilla Firefox Use-after-free in WebGPU IPC Framework
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

blogs

Reference: CVE-2022-26485
Description: Firefox in-the-wild 0day analysis
Link: https://weiyiling.cn/one/firefox_0day_case_analysis

Reference: CVE-2022-26485
Description: New details on commercial spyware vendor Variston
Link: https://blog.google/threat-analysis-group/new-details-on-commercial-spyware-vendor-variston/

Reference: CVE-2022-26486
Description: Firefox in-the-wild 0day analysis
Link: https://weiyiling.cn/one/firefox_0day_case_analysis

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

3 Mozilla Firefox Multiple Vulnerabilities (MFSA2022-10)

| | |
|---|---|
| QID: | 376458 |
| Category: | Local |
| Associated CVEs: | CVE-2022-26381, CVE-2022-26384, CVE-2022-26385, CVE-2022-26382, CVE-2022-0843, CVE-2022-26383, CVE-2022-26387 |
| Vendor Reference: | MFSA2022-10 |
| Bugtraq ID: | - |
| Service Modified: | 06/01/2023 |
| 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-2022-26383: Browser window spoof using fullscreen mode
CVE-2022-26384: iframe allow-scripts sandbox bypass
CVE-2022-26387: Time-of-check time-of-use bug when verifying add-on signatures
CVE-2022-26381: Use-after-free in text reflows
CVE-2022-26382: Autofill Text could be exfiltrated via side-channel attacks
CVE-2022-26385: Use-after-free in thread shutdown
CVE-2022-0843: Memory safety bugs fixed in Firefox 98
Affected Products:
Prior to Firefox 98

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 MFSA2022-10 or later (https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA2022-10 (https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2022-26384
Description: If an attacker could control the contents of an iframe sandboxed with allow-popups but not allow-scripts, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1744352

Reference: CVE-2022-26387
Description: When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1752979

Reference: CVE-2022-26381
Description: An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1736243

Reference: CVE-2022-26385
Description: In unusual circumstances, an individual thread may outlive the thread's manager during shutdown. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 98.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1747526

Reference: CVE-2022-26382
Description: While the text displayed in Autofill tooltips cannot be directly read by JavaScript, the text was rendered using page fonts. Side-channel attacks on the text by using specially crafted fonts could have lead to this text being inferred by the webpage. This vulnerability affects Firefox < 98.
Link: https://bugzilla.mozilla.org/show_bug.cgi?id=1741888

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 3 Mozilla Firefox Multiple Vulnerabilities (MFSA2015-93)

| | |
|---|---|
| QID: | 376496 |
| Category: | Local |
| Associated CVEs: | CVE-2015-4496 |
| Vendor Reference: | Mozilla |
| Bugtraq ID: | - |
| Service Modified: | 05/12/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Multiple integer overflows in libstagefright in Mozilla Firefox before 38.0 allow remote attackers to execute arbitrary code via crafted sample metadata in an MPEG-4 video file.

IMPACT:

Arbitrary code execution can lead to complete compromise of the system.

SOLUTION:

Update to Mozilla Firefox 38 or later, and SeaMonkey 2.35 or later.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
2015-93: Mozilla (Firefox) (https://www.mozilla.org/en-US/security/advisories/mfsa2015-93/)

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  1.7.0.0

### 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: | 12/21/2023 |
| 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.
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:

cisa-alerts

Reference: CVE-2023-4863
Description: CISA Adds Three Known Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2023/09/13/cisa-adds-three-known-vulnerabilities-catalog

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 WebP in Google Chrome prior to 116.0.5845.187 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/

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2023-4863
Type: Exploit
Platform: Image,Win32,Android

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 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: | 12/20/2023 |
| 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

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

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 2.0.0.0

## 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 2.0.0.0

## 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:

WIN10

### 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 Mozilla Firefox International Domain Name Subdomain URI Spoofing Vulnerability (MFSA 2009-15)

| | |
|---|---|
| QID: | 116233 |
| Category: | Local |
| Associated CVEs: | CVE-2009-0652 |
| Vendor Reference: | MFSA 2009-15 |
| Bugtraq ID: | 33837 |
| Service Modified: | 04/09/2009 |
| User Modified: | - |

| | |
|---|---|
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Mozilla Firefox is a browser available for a number of operating systems.
The application  is affected by a URI-spoofing vulnerability because it fails to adequately handle specific characters in IDN subdomains. Specifically, this issue results from the display of unspecified characters resembling the '/' forward slash character. An attacker may exploit this issue to create a subdomain which visually resembles a legitimate top level domain followed by additional information.
Firefox Versions 3.0.6 and prior are vulnerable.

IMPACT:

If this vulnerability is successfully exploited, attackers can spoof the source URI of a site presented to an unsuspecting user. This may lead to a false sense of trust because the user may be presented with a source URI of a trusted site while interacting with the attacker's malicious site.

SOLUTION:

Patch -
These vulnerabilities are fixed in Mozilla Firefox 3.0.9 and later. Firefox 3.0.9 is available for download at Mozilla Firefox Download site (http://www.mozilla.com/en-US/products/download.html?product=firefox-3.0.9&os=win&lang=en-US).
Refer to the following Mozilla Foundation security advisory for further details:
MFSA 2009-15 (http://www.mozilla.org/security/announce/2009/mfsa2009-15.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2009-15 (http://www.mozilla.org/security/announce/2009/mfsa2009-15.html)

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

### 2 Mozilla Firefox "designMode" Null Pointer Dereference Denial of Service Vulnerability

| | |
|---|---|
| QID: | 116243 |
| Category: | Local |
| Associated CVEs: | CVE-2009-0071 |
| Vendor Reference: | - |
| Bugtraq ID: | 33154 |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Mozilla Firefox is an open source Web browser.
A remote denial of service vulnerability exists in Firefox when the "document.designMode" property is set to "on". This issue is caused due to a null pointer dereference error in designMode which can be exploited by a malicious script code that can be used to delete an object and then call one of the "document.queryCommandValue()", "document.queryCommandState()", or "document.queryCommandIndexTerm()" functions to crash the browser.
Firefox Versions 3.0.5 and 3.0.6 are vulnerable; other versions may also be affected.

IMPACT:

If this vulnerability is successfully exploited, it will allow attackers to crash the affected browser, resulting in denial of service.

SOLUTION:

There are no vendor-supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference: CVE-2009-0071
Description: Mozilla Firefox 3.0.6 - BODY onload Remote Crash - The Exploit-DB Ref : 8091
Link: http://www.exploit-db.com/exploits/8091

exploitdb

Reference: CVE-2009-0071
Description: Mozilla Firefox 3.0.6 - BODY onload Remote Crash
Link: https://www.exploit-db.com/exploits/8091

nvd

Reference: CVE-2009-0071
Description: Mozilla Firefox 3.0.5 and earlier 3.0.x versions, when designMode is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a certain (a) replaceChild or (b) removeChild call, followed by a (1) queryCommandValue, (2) queryCommandState, or (3) queryCommandIndeterm call. NOTE: it was later reported that 3.0.6 and 3.0.7 are also affected.
Link: http://www.securityfocus.com/bid/33154

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 2 Mozilla Firefox XML Parser Denial of Service Vulnerability - Zero Day

| | |
|---|---|
| QID: | 116834 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 05/12/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Firefox is an open source Web browser application for multiple platforms.
Mozilla FireFox is exposed to a denial of service vulnerability due to memory corruption when handling specifically crafted XML document.
Mozilla FireFox version 3.6, 3.5.7 and 3.0.17 are affected by this issue. Other versions may also be affected.

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to cause denial of service like conditions.

SOLUTION:

There are no vendor supplied updates 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:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

 2 Mozilla Firefox and SeaMonkey Remote Denial of Service Vulnerability - Zero Day

| | |
|---|---|
| QID: | 116883 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | 38132 |
| Service Modified: | 05/12/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Firefox is an open source Web browser application for multiple platforms. SeaMonkey is an open source Web browser, email and newsgroup client, IRC chat client, and HTML editor.
Firefox and SeaMonkey are exposed to a remote denial of service vulnerability.
Affected Software:
Firefox 3.5.7, Firefox 3.0.17, Firefox 3.6, SeaMonkey 2.0.2 and prior

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to cause denial of service like conditions.

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:

%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe found
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

 2 Mozilla Firefox Click Jacking Vulnerability - Zero Day

| | |
|---|---|
| QID: | 116942 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 02/26/2010 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is an open source Web browser application for multiple platforms.
Mozilla Firefox is exposed to a click jacking vulnerability. An attacker can trick a user into visiting a malicious website through a seemingly innocuous web link.
Affected Software:
Firefox 3.5.8, Firefox 3.0.18, Firefox 3.6 and prior on Windows.

IMPACT:

Successfully exploiting this issue might allow a remote attacker to trick a user into visiting malicious web site.

SOLUTION:

There are no vendor supplied patches available at this point of time to address this issue.

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
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe Product Version is 1.7.0.0
%ProgramFiles(x86)%\Mozilla Firefox\firefox.exe  Version is  1.7.0.0

## 2 Mozilla Firefox Address Bar Spoofing Vulnerability

| | |
|---|---|
| QID: | 118145 |
| Category: | Local |
| Associated CVEs: | CVE-2010-1206 |
| Vendor Reference: | Firefox Bug 556957 |
| Bugtraq ID: | - |
| Service Modified: | 05/28/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is an open source Web browser application for multiple platforms.
Firefox is prone to an address bar spoofing vulnerability. When opening a page with window.open("hxxp://evil", "_blank"), the address bar will show hxxp://evil immediately, while the body still can be changed within the same origin of the opener.
By exploiting this vulnerability, the attacker can trick the user into believing they are visiting a legitimate site and conduct phishing attacks.

IMPACT:

By exploiting this vulnerability, the attacker can trick the user into believing they are visiting a legitimate site and conduct phishing attacks.

SOLUTION:

There are no vendor-supplied patches available at this time. Firefox has confirmed this issue and plans to fix it in Firefox 3.6.7. Please refer to Firefox Bug 556957 (https://bugzilla.mozilla.org/show_bug.cgi?id=556957) for details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2010-1206
Description: The startDocumentLoad function in browser/base/content/browser.js in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, does not properly implement the Same Origin Policy in certain circumstances related to the about:blank document and a document that is currently loading, which allows (1) remote web servers to conduct spoofing attacks via vectors involving a 204 (aka No Content) status code, and allows (2) remote attackers to conduct spoofing attacks via vec
Link: http://lcamtuf.blogspot.com/2010/06/yeah-about-that-address-bar-thing.html

Reference: CVE-2010-1206

Description: The startDocumentLoad function in browser/base/content/browser.js in Mozilla Firefox 3.5.x before 3.5.11 and 3.6.x before 3.6.7, and SeaMonkey before 2.0.6, does not properly implement the Same Origin Policy in certain circumstances related to the about:blank document and a document that is currently loading, which allows (1) remote web servers to conduct spoofing attacks via vectors involving a 204 (aka No Content) status code, and allows (2) remote attackers to conduct spoofing attacks via vec

Link: https://bugzilla.mozilla.org/show_bug.cgi?id=556957

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 2 Mozilla Firefox iFrame URL Protection Bypass Vulnerability

| | |
|---|---|
| QID: | 118406 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 08/18/2010 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is an open source Web browser application available for multiple Operating Systems.
Mozilla Firefox Web browser is exposed to a security bypass issue that could enable an attacker to trick a user into providing his login credentials for a given site by using an obfuscated URL.
Mozilla Firefox Version 3.6.8 is vulnerable. Other versions might also be affected.

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to bypass URL protections.

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:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

### 2 Mozilla Firefox Cache Objects History Enumeration Vulnerability - Zero Day

| | |
|---|---|
| QID: | 119769 |
| Category: | Local |
| Associated CVEs: | CVE-2011-4689 |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 05/29/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

A vulnerability in Mozilla Firefox, caused by an error when handling cache objects, can be exploited to enumerate visited sites.

Affected Versions:-
Mozilla Firefox versions 8.0.1 and earlier.

IMPACT:

An attacker can exploit this issue by enticing an unsuspecting victim to view a malicious webpage.

SOLUTION:

There are no vendor-supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2011-4689

Description: Microsoft Internet Explorer 6 through 9 does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.

Link: http://lcamtuf.coredump.cx/cachetime/

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 1.7.0.0

## 2 Mozilla Firefox/Thunderbird/SeaMonkey Clickjacking Vulnerability (MFSA2012-54)

| | |
|---|---|
| QID: | 372652 |
| Category: | Local |
| Associated CVEs: | CVE-2012-1964 |
| Vendor Reference: | MFSA2012-54 |
| Bugtraq ID: | - |
| Service Modified: | 06/03/2020 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is a browser. SeaMonkey is a suite of applications that includes a browser and an email client. Thunderbird is an email client.
Affected Versions:
Mozilla Firefox 4.x through 12.0
Firefox ESR 10.x prior to 10.0.6
Thunderbird 5.0 through 12.0
Thunderbird ESR 10.x before 10.0.6
SeaMonkey prior to 2.10

IMPACT:

Successful exploitation could allow man in the middle attack and attackers to trick users into adding an unintended exception via an IFRAME element.

SOLUTION:

Kindly refer to mfsa2012-54 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-54/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
mfsa2012-54 (https://www.mozilla.org/en-US/security/advisories/mfsa2012-54/)

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  1.7.0.0

2 Mozilla Firefox/Thunderbird Multiple Vulnerabilities (MFSA2010-43, MFSA2010-44, MFSA2010-34, MFSA2010-38)

| | |
|---|---|
| QID: | 372663 |
| Category: | Local |
| Associated CVEs: | CVE-2010-1207, CVE-2010-1210, CVE-2010-1215, CVE-2010-1211, CVE-2010-1212 |
| Vendor Reference: | mfsa2010-34, mfsa2010-38, mfsa2010-43, mfsa2010-44 |
| Bugtraq ID: | - |
| Service Modified: | 06/18/2021 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Firefox is is a free and open-source browser. Thunderbird is a free and open-source cross-platform email client developed for Windows, OS X, and Linux, with a mobile version for Android.
.
Affected versions:
Mozilla Firefox prior to 3.6.7
Thunderbird prior to 3.1.1

IMPACT:

Successful exploitation could allow remote attackers to obtain sensitive cross-origin information via vectors involving reference retention and node deletion.

SOLUTION:

Kindly refer to mfsa2010-43 (https://www.mozilla.org/en-US/security/advisories/mfsa2010-43/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2010-43 (https://www.mozilla.org/en-US/security/advisories/mfsa2010-43/)

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  1.7.0.0

1 Enabled Auto User Logon

| | |
|---|---|
| QID: | 90006 |
| Category: | Windows |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |

| | |
|---|---|
| Service Modified: | 01/05/2023 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

Microsoft Windows NT provides a feature called "Automatic logon", which allows a user to automatically log on to his local workstation without entering a password. This feature, while convenient, compromises the physical security of the workstation. Furthermore, it stores the autologin username and password in plaintext in the Windows registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

IMPACT:

Unauthorized users with physical access to the host can logon to the host with Administrator privileges or any other user.

SOLUTION:

We recommend that you locate the following key, and then set the value of the 'AutoAdminLogon' entry to '0':
Software\Microsoft\Windows%20NT\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 AutoAdminLogon = 1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon DefaultUserName exists.

## Potential Vulnerabilities (5)

### 3 Administrator Account's Password Does Not Expire

| | |
|---|---|
| QID: | 90080 |
| Category: | Windows |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 06/30/2023 |
| 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: 0 days, Last Password Set Date: (Wed 20 Dec 2023 11:56:08 PM GMT)

### 3 Pending Reboot Detected

| | |
|---|---|
| QID: | 90126 |
| Category: | Windows |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 06/22/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | Yes |

THREAT:

A pending reboot is detected at the host. This is normally set by the Microsoft Windows Installer after installing updates that need a reboot to complete.

IMPACT:

If this pending reboot is set by a Microsoft security patch, the host is probably still vulnerable to the security issues addressed by the patch, even though the registry may show that the patch is installed.

SOLUTION:

Reboot the machine.
Note: There is an issue with SQL Server 2000 Installer, which does not clear this pending reboot state after reboot and might give a false positive.

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\Component Based Servicing\RebootPending exists

### 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: | 11/23/2021 |
| 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.
Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

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 |

### 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:

DefaultAccount
Guest

## Information Gathered (164)

### 3 Accounts Enumerated From SAM Database Whose Passwords Do Not Expire

| | |
|---|---|
| QID: | 45031 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 08/31/2004 |
| 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

 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 |
|---|---|---|
| WIN10 | Workstation Service | 0x0 |
| WORKGROUP | Domain Name | 0x0 |
| WIN10 | File Server Service | 0x20 |
| WORKGROUP | Browser Service Elections | 0x1e |
| WORKGROUP | Master Browser | 0x1d |
| ..__MSBROWSE__. | Master Browser | 0x1 |

### 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 | | 542 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: | 05/11/2015 |
| 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\120.0.2210.77\BHO\ie_to_edge_bho_64.dll |
| Browser Helper Objects | |
| {1FD49718-1D00-4B19-AF5F-070AF6D5D54C} | C:\Program Files (x86)\Microsoft\Edge\Application\120.0.2210.77\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-1-5-21-3876893769-2693916039-3407467337-500", name="WIN10\\Administrator"}
Administrators {sid="S-1-5-21-3876893769-2693916039-3407467337-1000", name="WIN10\\vboxuser"}

### 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 read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
\SAMR AnonymousLogon 7 access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
\SAMR APPLICATION PACKAGE AUTHORITY\Your Windows credentials 8 access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
\SAMR Administrators 544 access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes

 3 Antivirus Product Detected on Windows Host

| | |
|---|---|
| QID: | 105327 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 07/19/2023 |
| 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

2 Operating System Detected

| | |
|---|---|
| QID: | 45017 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 12/18/2023 |
| 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 Home 64 bit Edition Version 22H2 | Windows Registry | |
| Windows 2016/2019/10 | NTLMSSP | |
| Windows 10 | TCP/IP Fingerprint | U7119:135 |
| cpe:/o:microsoft:windows_10:2009::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 | 4.8.09037 | 533325 | 4.8.1 - | HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Client |
| .Net Framework 4.x Full Installation x64 | 4.8.09037 | 533325 | 4.8.1 - | HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full |
| .Net Framework 4.x Client Installation x86 | 4.8.09037 | 533325 | 4.8.1 - | HKLM\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client |
| .Net Framework 4.x Full Installation x86 | 4.8.09037 | 533325 | 4.8.1 - | HKLM\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full |

 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 {sid="S-1-5-21-3876893769-2693916039-3407467337-500", name="WIN10\\Administrator", siduse="User"}
S-1-5-32-544 Administrators {sid="S-1-5-21-3876893769-2693916039-3407467337-1000", name="WIN10\\vboxuser", siduse="User"}

 2 Model Information from Devices

| | |
|---|---|
| QID: | 45304 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 11/13/2023 |
| 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 | = | d3e5cd87-8a05-482f-b373-cde32889990c |

 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 | 49670 | | | \PIPE\svcctl |
| Microsoft Spool Subsystem | 1.0 | 49668 | | | \PIPE\spoolss |
| Microsoft Task Scheduler | 1.0 | | | | \PIPE\atsvc |
| Microsoft Workstation Service | 1.0 | | | | \PIPE\wkssvc |
| RPC Browser | 0.0 | | | | \PIPE\browser |
| RPC ROUTER SERVICE | 1.0 | | | | \PIPE\ROUTER |
| 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 |
| Event log TCPIP | 1.0 | 49666 | | | \pipe\eventlog |
| (Unknown Service) | 1.0 | 49667 | | | \PIPE\atsvc |
| (Unknown Service) | 2.0 | | | | \PIPE\atsvc |
| (Unknown Service) | 1.0 | 49668 | | | |
| DfsDs service | 1.0 | | | | \PIPE\wkssvc |
| RemoteRegistry Perflib Interface | 1.0 | | | | \PIPE\winreg |
| Vpn APIs | 1.0 | | | | \PIPE\ROUTER |
| Remote Fw APIs | 1.0 | 49674 | | | |

 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 |
|---|---|---|---|---|---|---|
| Microsoft Update Health Tools | 3.74.0.0 | 20231220 | Microsoft Corporation | | | MsiExec.exe /X{1FC1A6C2-576E-489A-9B4A-92D21F542136} |
| Update for Windows 10 for x64-based Systems (KB5001716) | 8.93.0.0 | 20231220 | Microsoft Corporation | | | MsiExec.exe /X{7B63012A-4AC6-40C6-B6AF-B24A84359DD5} |
| Microsoft Edge | 120.0.2210.77 | 20231220 | Microsoft Corporation | | C:\Program Files (x86)\Microsoft\Edge\Application | "C:\Program Files (x86)\Microsoft\Edge\Application\120.0.2210.77\Installer\setup.exe" --uninstall --msedge --channel=stable --system-level --verbose-logging |
| Microsoft Edge Update | 1.3.181.5 | | | | | |
| Microsoft Edge WebView2 Runtime | 120.0.2210.77 | 20231220 | Microsoft Corporation | | C:\Program Files (x86)\Microsoft\EdgeWebView\Application | "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\120.0.2210.77\Installer\setup.exe" --uninstall --msedgewebview --system-level --verbose-logging |
| Mozilla Firefox (0.8.) | | | | | | C:\Windows\UninstallFirefox.exe /ua "0.8. (en)" |
| VLC media player 2.0.0 | 2.0.0 | | 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 8.110.19041.844
Microsoft XML parser (MSXML) v6 6.30.19041.1023
Microsoft XML parser (MSXML) v3 8.110.19041.844
Microsoft XML parser (MSXML) v6 6.30.19041.1081

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:

| S-1-5-32-551 |
|---|
| 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:

| S-1-5-32-551 |
|---|
| 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: | 03/22/2005 |
| 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: | 03/22/2005 |
| 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:
S-1-5-32-551
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:

| S-1-5-32-551 |
|---|
| 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 |
|---|
| S-1-5-32-551 |
| 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:

| S-1-5-32-551 |
| --- |
| Builtin\Users |
| BUILTIN\Administrators |
| WIN10\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:

| S-1-5-32-551 |
| --- |
| 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:
WIN10\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:
WIN10\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 |
|---|---|---|---|---|
| AudioEndpointBuilder | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| AudioEndpointBuilder | Access Allowed for Local_System | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-1-15-3-1024-1692970155-4054 893335-185714091-3362601943-3 526593181-1159816984-21990085 81-497492991 | standard-read | query-service-config | query-service-status |
| Audiosrv | Access Allowed for S-1-15-3-1024-1692970155-4054 893335-185714091-3362601943-3 526593181-1159816984-21990085 81-497492991 | 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 | - | - |
| Browser | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| Browser | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| Browser | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| Browser | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| Browser | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| Browser | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| Browser | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| Browser | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| Browser | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| Browser | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| Browser | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| BthAvctpSvc | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| BthAvctpSvc | Access Allowed for Local_System | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-1-15-3-1024-3203351429-2120443784-2872670797-1918958302-2829055647-4275794519-7656644 | enumerate-service-dependents | nterrogate-service | - |

| | | | | |
|---|---|---|---|---|
| | 14-2751773334 | | | |
| 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 |
| Dhcp | Access Allowed for Authenticated_Users | standard-read | query-service-config | query-service-status |
| Dhcp | Access Allowed for Authenticated_Users | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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 |
| DoSvc | Access Allowed for Authenticated_Users | standard-read | query-service-config | query-service-status |
| DoSvc | Access Allowed for Authenticated_Users | enumerate-service-dependents | start-service | nterrogate-service |
| DoSvc | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| DoSvc | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| DoSvc | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| DoSvc | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| DoSvc | Access Allowed for Local_System | standard-read | standard-write-owner | standard-write-dac |
| DoSvc | Access Allowed for Local_System | standard-delete | query-service-config | change-service-config |
| DoSvc | Access Allowed for Local_System | query-service-status | enumerate-service-dependents | start-service |
| DoSvc | Access Allowed for Local_System | stop-service | pause-continue-service | - |
| DoSvc | Access Allowed for S-1-5-80-3055155277-3816794035-3994065555-2874236192-2193176987 | standard-read | change-service-config | - |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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 | - | - |
| IKEEXT | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| IKEEXT | Access Allowed for Local_System | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | start-service | nterrogate-service |
| KeyIso | Access Allowed for Service_Logon | service-user-defined-control | - | - |
| KeyIso | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-1-15-3-1024-3842824567-178914259-466740046-159386189-423571359-3349026085-1947878110-3889710422 | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| LSM | Access Allowed for Authenticated_Users | query-service-config | query-service-status | enumerate-service-dependents |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents |
| 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-dependents | 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 |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| RasMan | Access Allowed for Authenticated_Users | standard-read | query-service-config | query-service-status |
| RasMan | Access Allowed for Authenticated_Users | enumerate-service-dependents | start-service | nterrogate-service |
| RasMan | Access Allowed for Authenticated_Users | service-user-defined-control | - | - |
| RasMan | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| RasMan | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| RasMan | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| RasMan | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| RasMan | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | standard-read | query-service-config | query-service-status |
| RasMan | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | enumerate-service-dependents | start-service | nterrogate-service |
| RasMan | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents |
| 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-dependents | 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-dependents |
| 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-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | standard-read | query-service-config | query-service-status |
| SecurityHealthService | Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | enumerate-service-dependents | start-service | stop-service |
| SecurityHealthService | Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | pause-continue-service | nterrogate-service | service-user-defined-control |
| SecurityHealthService | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-read | standard-write-owner | standard-write-dac |
| SecurityHealthService | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-delete | query-service-config | change-service-config |
| SecurityHealthService | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | query-service-status | enumerate-service-dependents | start-service |
| SecurityHealthService | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | stop-service | pause-continue-service | - |
| SecurityHealthService | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | standard-read | standard-write-owner | standard-write-dac |
| SecurityHealthService | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | standard-delete | query-service-config | change-service-config |
| SecurityHealthService | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | query-service-status | enumerate-service-dependents | start-service |
| SecurityHealthService | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | stop-service | pause-continue-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 |
| SstpSvc | Access Allowed for Authenticated_Users | standard-read | query-service-config | query-service-status |
| SstpSvc | Access Allowed for Authenticated_Users | enumerate-service-dependents | start-service | nterrogate-service |
| SstpSvc | Access Allowed for Authenticated_Users | service-user-defined-control | - | - |

| | | | | |
|---|---|---|---|---|
| SstpSvc | Access Allowed for Network_Configuration_Operators | standard-read | query-service-config | query-service-status |
| SstpSvc | Access Allowed for Network_Configuration_Operators | enumerate-service-dependents | start-service | stop-service |
| SstpSvc | Access Allowed for Network_Configuration_Operators | pause-continue-service | nterrogate-service | service-user-defined-control |
| SstpSvc | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| SstpSvc | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| SstpSvc | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| SstpSvc | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| SstpSvc | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| SstpSvc | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| SstpSvc | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| SstpSvc | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | standard-read | query-service-config | query-service-status |
| SstpSvc | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | enumerate-service-dependents | start-service | nterrogate-service |
| SstpSvc | Access Allowed for S-1-15-3-1024-1068037383-729401668-2768096886-125909118-1680096985-174794564-3112554050-3241210738 | service-user-defined-control | - | - |
| StateRepository | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-read | standard-write-owner | standard-write-dac |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| TrustedInstaller | Access Allowed for Local_System | standard-read | standard-write-owner | standard-write-dac |
| TrustedInstaller | Access Allowed for Local_System | standard-delete | query-service-config | change-service-config |
| TrustedInstaller | Access Allowed for Local_System | query-service-status | enumerate-service-dependents | start-service |
| TrustedInstaller | Access Allowed for Local_System | stop-service | pause-continue-service | - |
| TrustedInstaller | Access Allowed for Administrators | standard-read | query-service-config | change-service-config |
| TrustedInstaller | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| TrustedInstaller | Access Allowed for Administrators | stop-service | pause-continue-service | nterrogate-service |
| TrustedInstaller | Access Allowed for Administrators | service-user-defined-control | - | - |
| TrustedInstaller | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| TrustedInstaller | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| TrustedInstaller | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| TrustedInstaller | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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 | - |
| 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-1-5-80-2970612574-78537857-698502321-558674196-145164458 2 | standard-read | query-service-config | query-service-status |
| WdiServiceHost | Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-145164458 2 | enumerate-service-dependents | start-service | stop-service |
| WdiServiceHost | Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-145164458 2 | pause-continue-service | nterrogate-service | service-user-defined-control |

| | | | | |
|---|---|---|---|---|
| WdiSystemHost | Access Allowed for Local_System | standard-read | standard-write-owner | standard-write-dac |
| WdiSystemHost | Access Allowed for Local_System | standard-delete | query-service-config | change-service-config |
| WdiSystemHost | Access Allowed for Local_System | query-service-status | enumerate-service-dependents | start-service |
| WdiSystemHost | Access Allowed for Local_System | stop-service | pause-continue-service | - |
| WdiSystemHost | Access Allowed for Administrators | standard-read | query-service-config | change-service-config |
| WdiSystemHost | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | stop-service |
| WdiSystemHost | Access Allowed for Administrators | pause-continue-service | nterrogate-service | service-user-defined-control |
| WdiSystemHost | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| WdiSystemHost | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| WdiSystemHost | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| WdiSystemHost | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| WdiSystemHost | Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-1451644582 | standard-read | query-service-config | query-service-status |
| WdiSystemHost | Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-1451644582 | enumerate-service-dependents | start-service | stop-service |
| WdiSystemHost | Access Allowed for S-1-5-80-2970612574-78537857-698502321-558674196-1451644582 | pause-continue-service | nterrogate-service | service-user-defined-control |
| WdNisSvc | Access Allowed for Users | standard-read | query-service-config | query-service-status |
| WdNisSvc | Access Allowed for Users | enumerate-service-dependents | start-service | nterrogate-service |
| WdNisSvc | Access Allowed for Users | 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-dependents | start-service | nterrogate-service |
| WdNisSvc | Access Allowed for Local_System | service-user-defined-control | - | - |
| WdNisSvc | Access Allowed for Administrators | standard-read | query-service-config | query-service-status |
| WdNisSvc | Access Allowed for Administrators | enumerate-service-dependents | start-service | nterrogate-service |
| WdNisSvc | Access Allowed for Administrators | service-user-defined-control | - | - |
| WdNisSvc | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| WdNisSvc | Access Allowed for Interactive_Logon | enumerate-service-dependents | start-service | nterrogate-service |
| WdNisSvc | Access Allowed for Interactive_Logon | 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-dependents | start-service | nterrogate-service |
| WdNisSvc | Access Allowed for Service_Logon | service-user-defined-control | - | - |
| WdNisSvc | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | standard-read | standard-write-owner | standard-write-dac |
| WdNisSvc | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | standard-delete | query-service-config | change-service-config |
| WdNisSvc | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | query-service-status | enumerate-service-dependents | start-service |
| WdNisSvc | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | stop-service | pause-continue-service | - |
| WinDefend | Access Allowed for Users | standard-read | query-service-config | query-service-status |
| WinDefend | Access Allowed for Users | enumerate-service-dependents | start-service | nterrogate-service |
| WinDefend | Access Allowed for Users | service-user-defined-control | - | - |
| WinDefend | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| WinDefend | Access Allowed for Local_System | enumerate-service-dependents | start-service | nterrogate-service |
| WinDefend | Access Allowed for Local_System | service-user-defined-control | - | - |
| WinDefend | Access Allowed for Administrators | standard-read | query-service-config | query-service-status |
| WinDefend | Access Allowed for Administrators | enumerate-service-dependents | start-service | nterrogate-service |
| WinDefend | Access Allowed for Administrators | service-user-defined-control | - | - |

| | | | | |
|---|---|---|---|---|
| WinDefend | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| WinDefend | Access Allowed for Interactive_Logon | enumerate-service-dependents | 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 | - | - |
| WinDefend | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | standard-read | standard-write-owner | standard-write-dac |
| WinDefend | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | standard-delete | query-service-config | change-service-config |
| WinDefend | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | query-service-status | enumerate-service-dependents | start-service |
| WinDefend | Access Allowed for S-1-5-80-1913148863-3492339771-4165695881-2087618961-4109116736 | stop-service | pause-continue-service | - |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | start-service | nterrogate-service |
| wscsvc | Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | standard-read | query-service-config | query-service-status |
| wscsvc | Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | enumerate-service-dependents | start-service | stop-service |
| wscsvc | Access Allowed for S-1-5-80-1601830629-990752416-3372939810-977361409-3075122917 | pause-continue-service | nterrogate-service | service-user-defined-control |
| wscsvc | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-read | standard-write-owner | standard-write-dac |
| wscsvc | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-delete | query-service-config | change-service-config |
| wscsvc | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | query-service-status | enumerate-service-dependents | start-service |
| wscsvc | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | stop-service | pause-continue-service | - |
| wscsvc | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | standard-read | standard-write-owner | standard-write-dac |
| wscsvc | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | standard-delete | query-service-config | change-service-config |
| wscsvc | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | query-service-status | enumerate-service-dependents | start-service |
| wscsvc | Access Allowed for S-1-5-80-259296475-4084429506-1152984619-38739575-565535606 | stop-service | pause-continue-service | - |
| WSearch | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| WSearch | Access Allowed for Local_System | enumerate-service-dependents | 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 |
| WSearch | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| WSearch | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| WSearch | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| WSearch | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| WSearch | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |

| | | | | |
|---|---|---|---|---|
| WSearch | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| WSearch | Access Allowed for S-1-15-3-1024-724741592-12109 17904-489960769-637019204-334 5707629-3097053430-1727148295 -85063603 | standard-read | query-service-config | query-service-status |
| WSearch | Access Allowed for S-1-15-3-1024-724741592-12109 17904-489960769-637019204-334 5707629-3097053430-1727148295 -85063603 | enumerate-service-dependents | nterrogate-service | - |
| wuauserv | Access Allowed for Authenticated_Users | standard-read | query-service-config | query-service-status |
| wuauserv | Access Allowed for Authenticated_Users | enumerate-service-dependents | start-service | nterrogate-service |
| wuauserv | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| wuauserv | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| wuauserv | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| wuauserv | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| wuauserv | Access Allowed for Local_System | standard-read | standard-write-owner | standard-write-dac |
| wuauserv | Access Allowed for Local_System | standard-delete | query-service-config | change-service-config |
| wuauserv | Access Allowed for Local_System | query-service-status | enumerate-service-dependents | start-service |
| wuauserv | Access Allowed for Local_System | stop-service | pause-continue-service | - |
| cbdhsvc_6faaec | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| cbdhsvc_6faaec | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| cbdhsvc_6faaec | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| cbdhsvc_6faaec | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| cbdhsvc_6faaec | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| cbdhsvc_6faaec | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| cbdhsvc_6faaec | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| cbdhsvc_6faaec | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| cbdhsvc_6faaec | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| cbdhsvc_6faaec | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| cbdhsvc_6faaec | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| cbdhsvc_6faaec | Access Allowed for Authenticated_Users | service-user-defined-control | - | - |
| CDPUserSvc_6faaec | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| CDPUserSvc_6faaec | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| CDPUserSvc_6faaec | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| CDPUserSvc_6faaec | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| CDPUserSvc_6faaec | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| CDPUserSvc_6faaec | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| CDPUserSvc_6faaec | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| CDPUserSvc_6faaec | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| CDPUserSvc_6faaec | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| CDPUserSvc_6faaec | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| CDPUserSvc_6faaec | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| CDPUserSvc_6faaec | Access Allowed for Authenticated_Users | service-user-defined-control | - | - |
| OneSyncSvc_6faaec | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| OneSyncSvc_6faaec | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| OneSyncSvc_6faaec | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| OneSyncSvc_6faaec | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| OneSyncSvc_6faaec | Access Allowed for Local_System | standard-read | standard-write-owner | standard-write-dac |
| OneSyncSvc_6faaec | Access Allowed for Local_System | standard-delete | query-service-config | change-service-config |
| OneSyncSvc_6faaec | Access Allowed for Local_System | query-service-status | enumerate-service-dependents | start-service |
| OneSyncSvc_6faaec | Access Allowed for Local_System | stop-service | pause-continue-service | - |
| OneSyncSvc_6faaec | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |

Results were truncated.

| | |
|---|---|
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| CLFS | Access Allowed for S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464 | standard-read | standard-write-owner | standard-write-dac |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| fastfat | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| fastfat | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| fastfat | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| fastfat | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| fastfat | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| fastfat | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| fastfat | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| fastfat | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| fastfat | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| fastfat | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| fastfat | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |

| | | | | |
|---|---|---|---|---|
| fdc | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| fdc | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| fdc | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| fdc | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| fdc | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| fdc | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| fdc | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| fdc | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| fdc | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| fdc | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| fdc | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| flpydisk | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| flpydisk | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| flpydisk | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| flpydisk | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| flpydisk | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| flpydisk | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| flpydisk | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| flpydisk | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| flpydisk | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| flpydisk | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| flpydisk | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents |
| 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| mrxsmb10 | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| mrxsmb10 | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| mrxsmb10 | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| mrxsmb10 | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| mrxsmb10 | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| mrxsmb10 | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| mrxsmb10 | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| mrxsmb10 | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |

| | | | | |
|---|---|---|---|---|
| mrxsmb10 | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| mrxsmb10 | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| mrxsmb10 | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | start-service | stop-service |
| MsLldp | Access Allowed for System_Operators | pause-continue-service | nterrogate-service | service-user-defined-control |
| MsLldp | Access Allowed for S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453 | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | start-service | nterrogate-service |
| mssmbios | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| mssmbios | Access Allowed for Local_System | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| NdisTapi | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| NdisTapi | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| NdisTapi | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| NdisTapi | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| NdisTapi | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| NdisTapi | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| NdisTapi | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| NdisTapi | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| NdisTapi | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| NdisTapi | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| NdisTapi | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| NdisWan | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| NdisWan | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| NdisWan | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| NdisWan | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| NdisWan | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| NdisWan | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| NdisWan | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| NdisWan | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| NdisWan | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| NdisWan | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| NdisWan | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| ndproxy | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| ndproxy | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| ndproxy | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| ndproxy | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| ndproxy | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| ndproxy | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| ndproxy | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| ndproxy | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| ndproxy | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| ndproxy | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| ndproxy | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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_Operators | standard-read | query-service-config | query-service-status |
| NetBT | Access Allowed for Network_Configuration_Operators | enumerate-service-dependents | start-service | nterrogate-service |
| NetBT | Access Allowed for Network_Configuration_Operators | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| PptpMiniport | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| PptpMiniport | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| PptpMiniport | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| PptpMiniport | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| PptpMiniport | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| PptpMiniport | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| PptpMiniport | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| PptpMiniport | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| PptpMiniport | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| PptpMiniport | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| PptpMiniport | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | nterrogate-service | service-user-defined-control |
| RasAgileVpn | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| RasAgileVpn | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| RasAgileVpn | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| RasAgileVpn | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| RasAgileVpn | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| RasAgileVpn | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| RasAgileVpn | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| RasAgileVpn | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| RasAgileVpn | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| RasAgileVpn | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| RasAgileVpn | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| Rasl2tp | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| Rasl2tp | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| Rasl2tp | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| Rasl2tp | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| Rasl2tp | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| Rasl2tp | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| Rasl2tp | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| Rasl2tp | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| Rasl2tp | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| Rasl2tp | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| Rasl2tp | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| RasPppoe | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| RasPppoe | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| RasPppoe | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| RasPppoe | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| RasPppoe | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| RasPppoe | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| RasPppoe | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| RasPppoe | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| RasPppoe | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| RasPppoe | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| RasPppoe | Access Allowed for Service_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| RasSstp | Access Allowed for Local_System | standard-read | query-service-config | query-service-status |
| RasSstp | Access Allowed for Local_System | enumerate-service-dependents | start-service | stop-service |
| RasSstp | Access Allowed for Local_System | pause-continue-service | nterrogate-service | service-user-defined-control |
| RasSstp | Access Allowed for Administrators | standard-read | standard-write-owner | standard-write-dac |
| RasSstp | Access Allowed for Administrators | standard-delete | query-service-config | change-service-config |
| RasSstp | Access Allowed for Administrators | query-service-status | enumerate-service-dependents | start-service |
| RasSstp | Access Allowed for Administrators | stop-service | pause-continue-service | - |
| RasSstp | Access Allowed for Interactive_Logon | standard-read | query-service-config | query-service-status |
| RasSstp | Access Allowed for Interactive_Logon | enumerate-service-dependents | nterrogate-service | service-user-defined-control |
| RasSstp | Access Allowed for Service_Logon | standard-read | query-service-config | query-service-status |
| RasSstp | Access Allowed for Service_Logon | enumerate-service-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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-dependents | 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 |
| Results were truncated. | | | | |

2 Microsoft Windows Effective Permission on Shares Enumerated

| | |
|---|---|
| QID: | 105185 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 12/18/2020 |
| 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 |
| App Readiness | Manual | LocalSystem |
| AppX Deployment Service (AppXSVC) | 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 |
| Computer Browser | Manual | 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 |
| COM+ System Application | Manual | LocalSystem |
| CoreMessaging | Automatic | NT AUTHORITY\LocalService |
| Cryptographic Services | Automatic | NT Authority\NetworkService |
| DCOM Server Process Launcher | Automatic | LocalSystem |
| dcsvc | Manual | LocalSystem |

| | | |
|---|---|---|
| Optimize drives | Manual | localSystem |
| Device Association Service | Manual | 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 |
| 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 |
| 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 |
| 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 |
| 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 | Automatic | 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 |
| 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 | Automatic | localSystem |
| Auto Time Zone Updater | Disabled | NT AUTHORITY\LocalService |
| 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 |
| 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 |
| Microsoft Update Health Service | Disabled | LocalSystem |
| Agent Activation Runtime 6faaec | Manual | |
| GameDVR and Broadcast User Service 6faaec | Manual | |
| Bluetooth User Support Service 6faaec | Manual | |
| CaptureService 6faaec | Manual | |
| Clipboard User Service 6faaec | Manual | |
| Connected Devices Platform User Service 6faaec | Automatic | |
| ConsentUX 6faaec | Manual | |
| CredentialEnrollmentManagerUserSvc 6faaec | Manual | |
| DeviceAssociationBroker 6faaec | Manual | |
| DevicePicker 6faaec | Manual | |
| DevicesFlow 6faaec | Manual | |
| MessagingService 6faaec | Manual | |
| Sync Host 6faaec | Automatic | |
| Contact Data 6faaec | Manual | |
| PrintWorkflow 6faaec | Manual | |
| Udk User Service 6faaec | Manual | |
| User Data Storage 6faaec | Manual | |
| User Data Access 6faaec | Manual | |

| | |
|---|---|
| Windows Push Notifications User Service 6faaec | 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_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| ---------- | | |
| %windir%\AppPatch | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| %windir%\debug | | |
| ---------- | | |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed container_inherit object_inherit | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| %windir%\Help | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner |

| | | | |
|---|---|---|---|
| | | | standard_delete synchronize execute standard_write_dac write_extended_attr |
| Administrators | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | | |
| %windir%\inf | | | |
| ---------- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | | |
| %windir%\installer | | | |
| ---------- | | | |
| SYSTEM | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Everyone | access_allowed | container_inherit object_inherit | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Administrators | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| ---------- | | | |
| %windir%\media | | | |
| ---------- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac |

| | | | |
|---|---|---|---|
| | | | write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | | |
| %windir%\Registration | | | |
| ---------- | | | |
| Administrators | access_allowed | object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Everyone | access_allowed | object_inherit | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| ---------- | | | |
| %windir%\security | | | |
| ---------- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | | |
| %windir%\Temp | | | |
| ---------- | | | |
| Users | access_allowed | container_inherit | append_data write_data synchronize execute |

| | | |
|---|---|---|
| Administrators | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| ---------- | | |
| %ProgramFiles%\Common Files | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

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_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| %windir%\System32\ias | | | |
| Administrators | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| NETWORK_SERVICE | access_allowed | | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data synchronize execute write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| %windir%\System32\Config | | | |
| NT SERVICE\TrustedInstaller | access_allowed | container_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |

| | | | |
|---|---|---|---|
| SYSTEM | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| --- | | | |
| %windir%\System32\spool\printers | | | |
| --- | | | |
| Users | access_allowed | container_inherit | append_data read_attributes read_extended_attributes write_data synchronize |
| SYSTEM | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize standard_write_dac write_extended_attributes |
| Administrators | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize standard_write_dac write_extended_attributes |
| --- | | | |
| %windir%\System32\LogFiles | | | |
| --- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | | |
| %windir%\System32\inetsrv | | | |
| --- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |

| | | |
|---|---|---|
| SYSTEM | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

 2 Microsoft Windows File Security Check - C: System Files

| | |
|---|---|
| QID: | 105190 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 04/14/2006 |
| 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 | container_inherit | object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data |

| | | | |
|---|---|---|---|
| | | | read_data standard_write_owner<br>standard_delete synchronize execute<br>standard_write_dac<br>write_extended_attributes |
| SYSTEM | access_allowed | container_inherit object_inherit | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data<br>read_data standard_write_owner<br>standard_delete synchronize execute<br>standard_write_dac<br>write_extended_attributes |
| Users | access_allowed | container_inherit object_inherit | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| Authenticated_Users | access_allowed | | append_data |
| --- | | | |
| %ProgramFiles% | | | |
| --- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data<br>read_data standard_write_owner<br>standard_delete synchronize execute<br>standard_write_dac<br>write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes<br>read_attributes read_extended_attributes<br>write_data read_data standard_delete<br>synchronize execute<br>write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes<br>read_attributes read_extended_attributes<br>write_data read_data standard_delete<br>synchronize execute<br>write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| --- | | | |
| %CommonProgramFiles% | | | |
| --- | | | |
| NT SERVICE\TrustedInstaller | access_allowed | | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data<br>read_data standard_write_owner<br>standard_delete synchronize execute<br>standard_write_dac<br>write_extended_attributes |
| SYSTEM | access_allowed | | standard_read append_data write_attributes<br>read_attributes read_extended_attributes<br>write_data read_data standard_delete<br>synchronize execute<br>write_extended_attributes |
| Administrators | access_allowed | | standard_read append_data write_attributes<br>read_attributes read_extended_attributes<br>write_data read_data standard_delete<br>synchronize execute<br>write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | | standard_read read_attributes<br>read_extended_attributes read_data<br>synchronize execute |

## 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 | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Everyone | access_allowed | | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| %userprofile%\All Users | | | |
| SYSTEM | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |

| | | | |
|---|---|---|---|
| Administrators | access_allowed | container_inherit object_inherit | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | container_inherit object_inherit | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data synchronize execute write_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 read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Administrators access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\eventlog
---
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
NT SERVICE\EventLog access_allowed read_data standard_read append_data read_extended_attributes write_data read_attributes
Owner_Rights access_allowed read_data
---
\winreg
---
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
NT SERVICE\RemoteRegistry access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
Owner_Rights access_allowed standard_read
---
\srvsvc

---
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
SYSTEM access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\lsass
---
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Administrators access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\spoolss
---
Users access_allowed read_data write_data
Everyone access_allowed read_data write_extended_attributes standard_read write_attributes execute read_extended_attributes write_data read_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read write_attributes execute read_extended_attributes write_data read_attributes
Creator_Owner access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
SYSTEM access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
Administrators access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\svcctl
---
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Administrators access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\wkssvc
---
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
SYSTEM access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
NETWORK_SERVICE access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes
---
\NETLOGON
---
Everyone access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
AnonymousLogon access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
APPLICATION PACKAGE AUTHORITY\Your Windows credentials access_allowed read_data write_extended_attributes standard_read read_attributes read_extended_attributes write_data write_attributes
Administrators access_allowed read_data standard_read append_data standard_write_owner write_data write_attributes write_extended_attributes standard_delete read_attributes execute standard_write_dac delete_child read_extended_attributes

## 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
LastLoggedOnSAMUser = .\vboxuser
LastLoggedOnUser = .\vboxuser
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: | 08/04/2009 |
| 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 |
|---|---|
| 192.168.0.4 | No registered hostname |

1 Network Adapter MAC Address

| | |
|---|---|
| QID: | 43007 |
| Category: | Hardware |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 06/18/2020 |
| 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 | 08:00:27:4F:9D:04 | CADMUS COMPUTER SYSTEMS | | |
| #table | cols="5" | | | |
| DESCRIPTION | IP ADDRESS | MAC ADDRESS | Default IP Gateway | Subnet Mask |
| Intel(R) PRO/1000 MT Desktop Adapter | 192.168.0.4<br>fe80::bdea:f23c:c469:c261<br>2600:8801:208e:5200:8554:bc16:6ab9:f45f<br>2600:8801:208e:5200:4a13:6f75:d4d9:6e0f<br>2600:8801:208e:5200::3e41 | 08:00:27:4F:9D:04 | 192.168.0.1<br>fe80::8e6a:8dff:fe61:a71e | 255.255.255.0 64 128 64 128 |

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 69 Stepping 1, 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 | = | 4 |
| HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 | | |
| ProcessorNameString | = | Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz |

## 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 69 Stepping 1, 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 69 Stepping 1 |
| 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: 809 seconds

Start time: Thu, Dec 21 2023, 04:48:52 GMT

End time: Thu, Dec 21 2023, 05:02:21 GMT

## 1 Host Names Found

| | |
|---|---|
| QID: | 45039 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 08/27/2020 |
| 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 |
|---|---|
| win10 | NTLM DNS |
| WIN10 | NTLM NetBIOS |
| WIN10 | NetBIOS |
| WIN10 | 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: | 192.168.0.4 |

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C7F5787C-696D-44E6-B616-9B96B1EF2CB6}

| | | |
|---|---|---|
| EnableDHCP | = | 0 |
| Domain | = | |
| NameServer | = | |
| DhcpServer | = | 255.255.255.255 |
| SubnetMask | = | {"255.255.255.0"} |
| DefaultGateway | = | {"192.168.0.1"} |

1 Mozilla Firefox Web Browser Detected

| | |
|---|---|
| QID: | 45108 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 04/10/2020 |
| 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 = 0.8. (en)

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::bdea:f23c:c469:c261
2600:8801:208e:5200:8554:bc16:6ab9:f45f
2600:8801:208e:5200:4a13:6f75:d4d9:6e0f
2600:8801:208e:5200::3e41

## 1 System and BaseBoard Serial Numbers

| | |
|---|---|
| QID: | 45208 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 09/08/2021 |
| 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 : 0
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: | KB2677070, KB2813430 |
| 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 |
| 2796BAE63F1801E277261BA0D77770028F20EEE4 | Go Daddy Class 2 Certification Authority | Go Daddy Class 2 Certification Authority | 00 | 06/29/2004 | 06/29/2034 |
| 51501FBFCE69189D609CFAF140C576755DCC1FDF | Hotspot 2.0 Trust Root CA - 03 | Hotspot 2.0 Trust Root CA - 03 | 0cb30f70f286a433e0b90989de01edb7 | 12/08/2013 | 12/08/2043 |
| 5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25 | DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA | 02ac5c266a0b409b8f0b79f2ae462577 | 11/10/2006 | 11/10/2031 |

| | | | | | |
|---|---|---|---|---|---|
| | 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 |
| A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436 | DigiCert Global Root CA | DigiCert Global Root CA | 083be056904246b1a1756ac95991c74a | 11/10/2006 | 11/10/2031 |
| AD7E1C28B064EF8F6003402014C3D0E3370EB58A | Starfield Class 2 Certification Authority | Starfield Class 2 Certification Authority | 00 | 06/29/2004 | 06/29/2034 |
| B1BC968BD4F49D622AA89A81F2150152A41D829C | GlobalSign Root CA | GlobalSign Root CA | 040000000001154b5ac394 | 09/01/1998 | 01/28/2028 |
| B51C067CEE2B0C3DF855AB2D92F4FE39D4E70F0E | Starfield Root Certificate Authority - G2 | Starfield Root Certificate Authority - G2 | 00 | 09/01/2009 | 12/31/2037 |
| CABD2A79A1076A31F21D253635CB039D4329A5E8 | ISRG Root X1 | ISRG Root X1 | 8210cfb0d240e3594463e0bb63828b00 | 06/04/2015 | 06/04/2035 |
| D1EB23A46D17D68FD92564C2F1F1601764D8E349 | AAA Certificate Services | AAA Certificate Services | 01 | 01/01/2004 | 12/31/2028 |
| D4DE20D05E66FC53FE1A50882C78DB2852CAE474 | Baltimore CyberTrust Root | Baltimore CyberTrust Root | 020000b9 | 05/12/2000 | 05/12/2025 |
| D69B561148F01C77C54578C10926DF5B856976AD | GlobalSign | GlobalSign | 040000000000121585308a2 | 03/18/2009 | 03/18/2029 |
| DAC9024F54D8F6DF94935FB1732638CA6AD77C13 | DST Root CA X3 | DST Root CA X3 | 44afb080d6a327ba893039862ef8406b | 09/30/2000 | 09/30/2021 |
| DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 | DigiCert Global Root G2 | DigiCert Global Root G2 | 033af1e6a711a9a0bb2864b11d09fae5 | 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 |

| | | | | | |
|---|---|---|---|---|---|
| | Microsoft Root Certificate Authority 2010 | Microsoft Root Certificate Authority 2010 | 28cc3a25bfba44ac4 49a9b586b4339aa | 06/23/2010 | 06/23/2035 |
| 7F88CD7223F3C8138 18C994614A89C99FA 3B5247 | Microsoft Authenticode(tm) Root Authority | Microsoft Authenticode(tm) Root Authority | 01 | 01/01/1995 | 12/31/1999 |
| 8F43288AD272F3103 B6FB1428485EA3014 C0BCFE | Microsoft Root Certificate Authority 2011 | Microsoft Root Certificate Authority 2011 | 3f8bc8b5fc9fb2964 3b569d66c42e144 | 03/22/2011 | 03/22/2036 |
| 92B46C76E13054E10 4F230517E6E504D43 AB10B5 | Symantec Enterprise Mobile Root for Microsoft | Symantec Enterprise Mobile Root for Microsoft | 0f6b552f9ebf907b0 f6629a9bdf4d8ce | 03/15/2012 | 03/14/2032 |
| A43489159A520F0D9 3D032CCAF37E7FE20 A8B419 | Microsoft Root Authority | Microsoft Root Authority | c1008b3c3c8811d13 ef663ecdf40 | 01/10/1997 | 12/31/2020 |
| BE36A4562FB2EE05D BB3D32323ADF44508 4ED656 | Thawte Timestamping CA | Thawte Timestamping CA | 00 | 01/01/1997 | 12/31/2020 |
| CDD4EEAE6000AC7F4 0C3802C171E301480 30C072 | Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 79ad16a14aa0a5ad4 c7358f407132e65 | 05/09/2001 | 05/09/2021 |

## 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 | 192.168.0.4<br>fe80::bdea:f23c:c469:c261<br>2600:8801:208e:5200:8554:bc16:6ab9:f45f<br>2600:8801:208e:5200:4a13:6f75:d4d9:6e0f<br>2600:8801:208e:5200::3e41 | 08:00:27:4F:9D:04 | 192.168.0.1<br>fe80::8e6a:8dff:fe61:a71e | 255.255.255.0 64 128 64 128 |

## 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 1 Enabled

| | |
|---|---|
| QID: | 45261 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | SMB v1 |
| Bugtraq ID: | - |
| Service Modified: | 09/19/2019 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
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-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CAPTION INSTALLSTATE NAME
SMB 1.0/CIFS File Sharing Support 1 SMB1Protocol
SMB Server version 1 is Enabled
HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10 Start = 2
SMB Client version 1 is Enabled

 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  120.0.2210.77

 1 System Management BIOS UUID Detected

| | |
|---|---|
| QID: | 45303 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 07/11/2023 |
| 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 : 0BAD6026-56CD-45F7-A030-0F364EAD8B44

 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: | 04/17/2020 |
| 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 Home
ReleaseId = 2009

 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 = Pacific Standard Time
UTC = -08:00

 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: | 12/04/2019 |
| 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_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| C:\\Windows\\System32\\alg.exe | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| C:\\Windows\\System32\\svchost.exe | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| C:\\Windows\\system32\\dllhost.exe | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| ---------- | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| C:\\Windows\\system32\\DiagSvcs\\DiagnosticsHub.StandardCollector.Service.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Program Files (x86)\\Microsoft\\EdgeUpdate\\MicrosoftEdgeUpdate.exe | | |
| ---------- | | |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\System32\\lsass.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\system32\\fxssvc.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| --- | | |
| C:\\Windows\\system32\\lsass.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\120.0.2210.77\\elevation_service.exe | | |
| --- | | |
| S-1-15-3-1024-3635283841-2530182609-996808640-1887759898-3848208603-3313616867-983405619-2501854204 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Restricted_Code | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| S-1-15-2-543634040-274359014-2226501544-3561766748-3991453649-3543631192-522786984 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| S-1-15-3-1024-3424233489-972189580-2057154623-747635277-1604371224-316187997-3786583170-1043257646 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| S-1-15-3-1024-2302894289-466761758-1166120688-1039016420-2430351297-4240214049-4028510897-3317428798 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Administrators | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| --- | | |
| C:\\Windows\\System32\\msdtc.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\msiexec.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes |

| | | |
|---|---|---|
| | | read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\Microsoft.NET\\Framework 64\\v4.0.30319\\SMSvcHost.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\PerceptionSimulation\\PerceptionSimulationService.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\SysWow64\\perfhost.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\locator.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |

| | | |
|---|---|---|
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\SecurityHealthService.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\System32\\SensorDataService.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\SgrmBroker.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\System32\\snmptrap.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| ---------- | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| C:\\Windows\\system32\\spectrum.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\System32\\spoolsv.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\system32\\sppsvc.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\System32\\OpenSSH\\ssh-agent.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| ---------- | | |
| C:\\Windows\\system32\\TieringEngineService.exe | | |
| ---------- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes |

| | | |
|---|---|---|
| | | read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\servicing\\TrustedInstaller.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\System32\\vds.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\vssvc.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\wbengine.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child<br>write_attributes read_attributes<br>read_extended_attributes write_data read_data<br>standard_write_owner standard_delete synchronize<br>execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.18.23110.3-0\\NisSrv.exe | | |
| --- | | |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| --- | | |
| C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.18.23110.3-0\\MsMpEng.exe | | |
| --- | | |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| S-1-15-3-1024-3153509613-960666767-3724611135-2725662640-12138253-543910227-1950414635-4190290187 | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read append_data write_attributes read_attributes read_extended_attributes write_data read_data standard_delete synchronize execute write_extended_attributes |
| --- | | |
| C:\\Windows\\system32\\wbem\\WmiApSrv.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

| | | |
|---|---|---|
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed<br>access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute<br>standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Program Files\\Windows Media Player\\wmpnetwk.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\SearchIndexer.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Program Files\\Microsoft Update Health Tools\\uhssvc.exe | | |
| --- | | |
| SYSTEM | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| --- | | |
| C:\\Windows\\system32\\CredentialEnrollmentManager.exe | | |
| --- | | |
| NT SERVICE\TrustedInstaller | access_allowed | standard_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes |
| Administrators | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| SYSTEM | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| Users | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |
| APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES | access_allowed | standard_read read_attributes read_extended_attributes read_data synchronize execute |

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 | 0:02:59 |
| TCP | 139 | 0:00:18 |
| TCP | 445 | 0:20:13 |
| UDP | 137 | 0:01:02 |
| UDP | 138 | 0:00:09 |
| UDP | 500 | 0:00:12 |
| UDP | 1900 | 0:00:14 |

 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 = vboxuser

 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: | 11/29/2023 |
| 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 : 4
LogicalProcessors : 4
MultiThreading is Not Enabled

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 | ExecutablePath | ExecutionState | InstallDate | ProcessId | TerminationDate |
|---|---|---|---|---|---|---|---|---|---|
| System Idle Process | N/A | System Idle Process | 20231220204616.544983-480 | System Idle Process | N/A | N/A | N/A | 0 | N/A |
| System | N/A | System | 20231220204616.544983-480 | System | N/A | N/A | N/A | 4 | N/A |
| Registry | N/A | Registry | 20231220204610.863470-480 | Registry | N/A | N/A | N/A | 108 | N/A |
| smss.exe | N/A | smss.exe | 20231220204616.560683-480 | smss.exe | N/A | N/A | N/A | 400 | N/A |
| csrss.exe | N/A | csrss.exe | 20231220204630.819277-480 | csrss.exe | N/A | N/A | N/A | 496 | N/A |
| wininit.exe | N/A | wininit.exe | 20231220204631.273903-480 | wininit.exe | N/A | N/A | N/A | 572 | N/A |
| services.exe | N/A | services.exe | 20231220204631.506890-480 | services.exe | N/A | N/A | N/A | 644 | N/A |
| lsass.exe | C:\Windows\system32\lsass.exe | lsass.exe | 20231220204631.881790-480 | lsass.exe | C:\Windows\system32\lsass.exe | N/A | N/A | 716 | N/A |
| fontdrvhost.exe | "fontdrvhost.exe" | fontdrvhost.exe | 20231220204632.754101-480 | fontdrvhost.exe | C:\Windows\system32\fontdrvhost.exe | N/A | N/A | 892 | N/A |
| Memory Compression | N/A | Memory Compression | 20231220204634.713943-480 | Memory Compression | N/A | N/A | N/A | 1776 | N/A |
| spoolsv.exe | C:\Windows\System32\spoolsv.exe | spoolsv.exe | 20231220204635.854089-480 | spoolsv.exe | C:\Windows\System32\spoolsv.exe | N/A | N/A | 2568 | N/A |
| MsMpEng.exe | N/A | MsMpEng.exe | 20231220204637.934534-480 | MsMpEng.exe | N/A | N/A | N/A | 3100 | N/A |
| SearchIndexer.exe | C:\Windows\system32\SearchIndexer.exe /Embedding | SearchIndexer.exe | 20231220204739.979268-480 | SearchIndexer.exe | C:\Windows\system32\SearchIndexer.exe | N/A | N/A | 4100 | N/A |
| NisSrv.exe | N/A | NisSrv.exe | 20231220204739.993000-480 | NisSrv.exe | N/A | N/A | N/A | 704 | N/A |
| MoUsoCoreWorker.exe | C:\Windows\System32\mousocoreworker.exe -Embedding | MoUsoCoreWorker.exe | 20231220204746.593239-480 | MoUsoCoreWorker.exe | C:\Windows\System32\mousocoreworker.exe | N/A | N/A | 1428 | N/A |
| SecurityHealthService.exe | N/A | SecurityHealthService.exe | 20231220204749.760046-480 | SecurityHealthService.exe | N/A | N/A | N/A | 924 | N/A |
| SgrmBroker.exe | N/A | SgrmBroker.exe | 20231220204840.481618-480 | SgrmBroker.exe | N/A | N/A | N/A | 6232 | N/A |
| wuauclt.exe | "C:\Windows\system32\wuauclt.exe" /UpdateDeploymentProvider UpdateDeploymentProvider.d | wuauclt.exe | 20231220205156.020346-480 | wuauclt.exe | C:\Windows\system32\wuauclt.exe | N/A | N/A | 6752 | N/A |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | ll /ClassId c96de80b-2ee6-48ed-8517-efeda81d51cc /RunHandlerComServer | | | | | | | | |
| TrustedInstaller.exe | C:\Windows\servicing\TrustedInstaller.exe | TrustedInstaller.exe | 20231220205158.594026-480 | TrustedInstaller.exe | C:\Windows\servicing\TrustedInstaller.exe | N/A | N/A | 1684 | N/A |
| TiWorker.exe | C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3745_none_7ded3f327ca60a41\TiWorker.exe -Embedding | TiWorker.exe | 20231220205215.170273-480 | TiWorker.exe | C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.3745_none_7ded3f327ca60a41\TiWorker.exe | N/A | N/A | 7156 | N/A |
| csrss.exe | N/A | csrss.exe | 20231220211421.364076-480 | csrss.exe | N/A | N/A | N/A | 5784 | N/A |
| winlogon.exe | winlogon.exe | winlogon.exe | 20231220211421.564078-480 | winlogon.exe | C:\Windows\system32\winlogon.exe | N/A | N/A | 6964 | N/A |
| fontdrvhost.exe | "fontdrvhost.exe" | fontdrvhost.exe | 20231220211422.565190-480 | fontdrvhost.exe | C:\Windows\system32\fontdrvhost.exe | N/A | N/A | 2592 | N/A |
| dwm.exe | "dwm.exe" | dwm.exe | 20231220211423.092049-480 | dwm.exe | C:\Windows\system32\dwm.exe | N/A | N/A | 1136 | N/A |
| sihost.exe | sihost.exe | sihost.exe | 20231220211924.881999-480 | sihost.exe | C:\Windows\system32\sihost.exe | N/A | N/A | 7728 | N/A |
| taskhostw.exe | taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E} | taskhostw.exe | 20231220211925.479889-480 | taskhostw.exe | C:\Windows\system32\taskhostw.exe | N/A | N/A | 7376 | N/A |
| explorer.exe | C:\Windows\Explorer.EXE | explorer.exe | 20231220211928.753075-480 | explorer.exe | C:\Windows\Explorer.EXE | N/A | N/A | 4760 | N/A |
| StartMenuExperienceHost.exe | "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca | StartMenuExperienceHost.exe | 20231220211936.413205-480 | StartMenuExperienceHost.exe | C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe | N/A | N/A | 4848 | N/A |
| RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe -Embedding | RuntimeBroker.exe | 20231220211937.214912-480 | RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe | N/A | N/A | 7176 | N/A |
| SearchApp.exe | "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca | SearchApp.exe | 20231220211938.775904-480 | SearchApp.exe | C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe | N/A | N/A | 4208 | N/A |
| RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe -Embedding | RuntimeBroker.exe | 20231220211939.540272-480 | RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe | N/A | N/A | 2884 | N/A |
| ctfmon.exe | "ctfmon.exe" | ctfmon.exe | 20231220211941.192025-480 | ctfmon.exe | C:\Windows\system32\ctfmon.exe | N/A | N/A | 8300 | N/A |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | "C:\Windows\System32\SecurityHealthSystray.exe" | SecurityHealthSystray.exe | 20231220211951.837904-480 | SecurityHealthSystray.exe | C:\Windows\System32\SecurityHealthSystray.exe | N/A | N/A | 8816 | N/A |
| PhoneExperienceHost.exe | "C:\Program Files\WindowsApps\Microsoft.YourPhone_1.23102.126.0_x64__8wekyb3d8bbwe\PhoneExperienceHost.exe" -ComServer:Background -Embedding | PhoneExperienceHost.exe | 20231220211958.878814-480 | PhoneExperienceHost.exe | C:\Program Files\WindowsApps\Microsoft.YourPhone_1.23102.126.0_x64__8wekyb3d8bbwe\PhoneExperienceHost.exe | N/A | N/A | 9212 | N/A |
| RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe -Embedding | RuntimeBroker.exe | 20231220212011.129110-480 | RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe | N/A | N/A | 9056 | N/A |
| WmiPrvSE.exe | C:\Windows\system32\wbem\wmiprvse.exe | WmiPrvSE.exe | 20231220212047.690385-480 | WmiPrvSE.exe | C:\Windows\system32\wbem\wmiprvse.exe | N/A | N/A | 6784 | N/A |
| WmiPrvSE.exe | C:\Windows\system32\wbem\wmiprvse.exe | WmiPrvSE.exe | 20231220212114.299412-480 | WmiPrvSE.exe | C:\Windows\system32\wbem\wmiprvse.exe | N/A | N/A | 8600 | N/A |
| taskhostw.exe | taskhostw.exe | taskhostw.exe | 20231220212139.617501-480 | taskhostw.exe | C:\Windows\system32\taskhostw.exe | N/A | N/A | 300 | N/A |
| ShellExperienceHost.exe | "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca | ShellExperienceHost.exe | 20231220212141.494744-480 | ShellExperienceHost.exe | C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe | N/A | N/A | 8508 | N/A |
| RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe -Embedding | RuntimeBroker.exe | 20231220212143.542966-480 | RuntimeBroker.exe | C:\Windows\System32\RuntimeBroker.exe | N/A | N/A | 4116 | N/A |
| svchost.exe | C:\Windows\system32\svchost.exe -k DcomLaunch -p | svchost.exe | 20231220204632.708620-480 | svchost.exe | C:\Windows\system32\svchost.exe | N/A | N/A | 856 | 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 |
|---|---|---|
| Microsoft Update Health Tools | 3.74.0.0 | HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1FC1A6C2-576E-489A-9B4A-92D21F542136} |
| Update for Windows 10 for x64-based Systems (KB5001716) | 8.93.0.0 | HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{7B63012A-4AC6-40C6-B6AF-B24A84359DD5} |
| Microsoft Edge | 120.0.2210.77 | HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Edge |
| Microsoft Edge Update | 1.3.181.5 | HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Edge Update |
| Microsoft Edge WebView2 Runtime | 120.0.2210.77 | HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft EdgeWebView |
| Mozilla Firefox (0.8.) | | HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox (0.8.) |
| VLC media player 2.0.0 | 2.0.0 | 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 10.0.19041.2965

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 | = | 4 |

1 Microsoft Windows Status of FIPS Algorithm Policy

| | |
|---|---|
| QID: | 45567 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | FipsAlgorithmPolicy |
| Bugtraq ID: | - |
| Service Modified: | 03/21/2023 |
| 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:

vboxuser
HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastLoggedOnSAMUser = .\vboxuser
LastLoggedOnUser = .\vboxuser
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: | 12/11/2023 |
| 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 Windows Host Environment Variables Detected

| | |
|---|---|
| QID: | 48196 |
| Category: | Information gathering |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 10/17/2022 |
| 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 = 4
PROCESSOR_LEVEL = 6
PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 69 Stepping 1, GenuineIntel
PROCESSOR_REVISION = 4501
---

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 |
|---|---|---|
| Administrators | : | Administrator, vboxuser, |
| Device Owners | : | |
| Distributed COM Users | : | |
| Event Log Readers | : | |
| Guests | : | Guest, |
| Hyper-V Administrators | : | |
| IIS_IUSRS | : | IUSR, |
| Performance Log Users | : | |
| Performance Monitor Users | : | |
| Remote Management Users | : | |
| System Managed Accounts Group | : | DefaultAccount, |
| Users | : | INTERACTIVE, Authenticated Users, vboxuser, |

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 for Windows 10 | 0 | 3 |
| Microsoft XPS Document Writer | 0 | 3 |
| Microsoft Print to PDF | 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: | 09/04/2023 |
| 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
Microsoft.549981C3F5F10 4.2308.1005.0 C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_4.2308.1005.0_neutral_~_8wekyb3d8bbwe\
Microsoft.BingWeather 4.25.20211.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.BingWeather_4.25.20211.0_neutral_~_8wekyb3d8bbwe\
Microsoft.DesktopAppInstaller 2023.1215.611.0 C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_2023.1215.611.0_neutral_~_8wekyb3d8bbwe\
Microsoft.GetHelp 10.2308.12552.0 C:\Program Files\WindowsApps\Microsoft.GetHelp_10.2308.12552.0_neutral_~_8wekyb3d8bbwe\
Microsoft.Getstarted 2021.2309.0.0 C:\Program Files\WindowsApps\Microsoft.Getstarted_2021.2309.0.0_neutral_~_8wekyb3d8bbwe\
Microsoft.HEIFImageExtension 1.0.22742.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.HEIFImageExtension_1.0.22742.0_x64__8wekyb3d8bbwe\
Microsoft.Microsoft3DViewer 2023.2311.30032.0 C:\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_2023.2311.30032.0_neutral_~_8wekyb3d8bbwe\
Microsoft.MicrosoftEdge.Stable 92.0.902.67 C:\Program Files\WindowsApps\Microsoft.MicrosoftEdge.Stable_92.0.902.67_neutral__8wekyb3d8bbwe\
Microsoft.MicrosoftOfficeHub 18.2306.1061.0 C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2306.1061.0_neutral_~_8wekyb3d8bbwe\
Microsoft.MicrosoftSolitaireCollection 4.4.8204.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_4.4.8204.0_neutral_~_8wekyb3d8bbwe\
Microsoft.MicrosoftStickyNotes 3.6.73.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MicrosoftStickyNotes_3.6.73.0_neutral_~_8wekyb3d8bbwe\
Microsoft.MixedReality.Portal 2000.21051.1282.0 C:\Program Files\WindowsApps\Microsoft.MixedReality.Portal_2000.21051.1282.0_neutral_~_8wekyb3d8bbwe\
Microsoft.MSPaint 2019.729.2301.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.MSPaint_2019.729.2301.0_neutral_~_8wekyb3d8bbwe\
Microsoft.Office.OneNote 16001.14326.21738.0 C:\Program Files\WindowsApps\Microsoft.Office.OneNote_16001.14326.21738.0_neutral_~_8wekyb3d8bbwe\
Microsoft.People 2021.2202.33.0 C:\Program Files\WindowsApps\Microsoft.People_2021.2202.33.0_neutral_~_8wekyb3d8bbwe\
Microsoft.ScreenSketch 2021.2008.3001.0 C:\Program Files\WindowsApps\Microsoft.ScreenSketch_2021.2008.3001.0_neutral_~_8wekyb3d8bbwe\
Microsoft.SkypeApp 15.110.3218.0 C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.110.3218.0_neutral_~_kzf8qxf38zg5c\
Microsoft.StorePurchaseApp 22310.1401.1.0 C:\Program Files\WindowsApps\Microsoft.StorePurchaseApp_22310.1401.1.0_neutral_~_8wekyb3d8bbwe\
Microsoft.VCLibs.140.00 14.0.32530.0 C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.32530.0_x64__8wekyb3d8bbwe\
Microsoft.VP9VideoExtensions 1.0.22681.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe\
Microsoft.Wallet 2.4.18324.0 %SYSTEMDRIVE%\Program Files\WindowsApps\Microsoft.Wallet_2.4.18324.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WebMediaExtensions 1.0.62931.0 C:\Program Files\WindowsApps\Microsoft.WebMediaExtensions_1.0.62931.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WebpImageExtension 1.0.62681.0 C:\Program Files\WindowsApps\Microsoft.WebpImageExtension_1.0.62681.0_neutral_~_8wekyb3d8bbwe\
Microsoft.Windows.Photos 2019.19071.12548.0 C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsAlarms 2022.2306.23.0 C:\Program Files\WindowsApps\Microsoft.WindowsAlarms_2022.2306.23.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsCalculator 2021.2307.4.0 C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_2021.2307.4.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsCamera 2022.2311.5.0 C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2022.2311.5.0_neutral_~_8wekyb3d8bbwe\
microsoft.windowscommunicationsapps 16005.14326.21768.0 C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.21768.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsFeedbackHub 2023.928.751.0 C:\Program Files\WindowsApps\Microsoft.WindowsFeedbackHub_2023.928.751.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsMaps 2022.2311.1.0 C:\Program Files\WindowsApps\Microsoft.WindowsMaps_2022.2311.1.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsSoundRecorder 2021.2103.28.0 C:\Program Files\WindowsApps\Microsoft.WindowsSoundRecorder_2021.2103.28.0_neutral_~_8wekyb3d8bbwe\
Microsoft.WindowsStore 22311.1401.2.0 C:\Program Files\WindowsApps\Microsoft.WindowsStore_22311.1401.2.0_neutral_~_8wekyb3d8bbwe\
Microsoft.Xbox.TCUI 1.24.10001.0 C:\Program Files\WindowsApps\Microsoft.Xbox.TCUI_1.24.10001.0_neutral_~_8wekyb3d8bbwe\
Microsoft.XboxApp 48.104.4001.0 C:\Program Files\WindowsApps\Microsoft.XboxApp_48.104.4001.0_neutral_~_8wekyb3d8bbwe\
Microsoft.XboxGameOverlay 1.54.4001.0 C:\Program Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_neutral_~_8wekyb3d8bbwe\
Microsoft.XboxGamingOverlay 6.123.11012.0 C:\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_6.123.11012.0_neutral_~_8wekyb3d8bbwe\
Microsoft.XboxIdentityProvider 12.95.3001.0 C:\Program Files\WindowsApps\Microsoft.XboxIdentityProvider_12.95.3001.0_neutral_~_8wekyb3d8bbwe\
Microsoft.XboxSpeechToTextOverlay 1.21.13002.0 C:\Program Files\WindowsApps\Microsoft.XboxSpeechToTextOverlay_1.21.13002.0_neutral_~_8wekyb3d8bbwe\
Microsoft.YourPhone 1.23102.126.0 C:\Program Files\WindowsApps\Microsoft.YourPhone_1.23102.126.0_neutral_~_8wekyb3d8bbwe\
Microsoft.ZuneMusic 11.2310.8.0 C:\Program Files\WindowsApps\Microsoft.ZuneMusic_11.2310.8.0_neutral_~_8wekyb3d8bbwe\
Microsoft.ZuneVideo 2019.22091.10051.0 C:\Program Files\WindowsApps\Microsoft.ZuneVideo_2019.22091.10051.0_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 | vboxuser |
| Domain | (none) |
| Authentication Scheme | NTLMSSP v2 |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Discovery Method | Login credentials provided by user |
| CIFS Signing | default |
| Authentication Record | win10credentialed |
| CIFS Version | SMB v3.1.1 |

## 1 Windows Login User Information

| | |
|---|---|
| QID: | 70035 |
| Category: | SMB / NETBIOS |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 02/26/2004 |
| 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: | vboxuser |
| Full name: | vboxuser |
| Home directory: | |
| Home drive: | |
| Account description: | |
| Last logon: | Thu Dec 21 05:26:21 2023 |

| | |
|---|---|
| Password last set: | Wed Dec 20 23:56:08 2023 |
| Password must change: | Wed Jan 31 23:56:08 2024 |
| Member of | |
| | |
| None | |

1 Windows Authentication Method for User-Provided Credentials

| | |
|---|---|
| QID: | 70053 |
| Category: | SMB / NETBIOS |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 11/06/2009 |
| 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 | vboxuser |
| Domain | (none) |
| Authentication Scheme | NTLMSSP v2 |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Authentication Record | win10credentialed |

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: | 11/20/2023 |
| 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 | 05:25:21 GMT |
| Unreachable (type=3 code=3) | UDP Port 1 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 31785 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 5400 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 7938 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 1812 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 13 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 1044 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 121 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 7307 | Port Unreachable |
| Unreachable (type=3 code=3) | UDP Port 1035 | Port Unreachable |
| Unreachable (type=3 code=2) | IP with High Protocol | Protocol Unreachable |

## 1 NetBIOS Host Name

| | |
|---|---|
| QID: | 82044 |
| Category: | TCP/IP |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/21/2005 |
| 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:

WIN10

 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 1923249459 with a standard deviation of -2147483648. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(109090 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 2 2 2 2 2 2 2 2 3
Duration: 792 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: | 01/14/2005 |
| 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: | 08/29/2003 |
| 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: | 08/29/2003 |
| 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 | | Application Information |
| AppReadiness | | App Readiness |
| AppXSvc | | AppX Deployment Service (AppXSVC) |
| 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 |
| Browser | started | Computer Browser |
| 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) |
| COMSysApp | | COM+ System Application |
| CoreMessagingRegistrar | started | CoreMessaging |
| CryptSvc | started | Cryptographic Services |
| DcomLaunch | started | DCOM Server Process Launcher |
| dcsvc | | dcsvc |
| defragsvc | | Optimize drives |
| DeviceAssociationService | | 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 |
| 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 | started | 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 | | Function Discovery Provider Host |

| | | |
|---|---|---|
| FDResPub | | Function Discovery Resource Publication |
| fhsvc | | File History Service |
| FontCache | started | Windows Font Cache Service |
| FrameServer | | Windows Camera Frame Server |
| gpsvc | | 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 |
| NaturalAuthentication | | Natural Authentication |
| NcaSvc | | Network Connectivity Assistant |
| NcbService | started | Network Connection Broker |
| NcdAutoSetup | | Network Connected Devices Auto-Setup |
| Netlogon | | Netlogon |
| Netman | | 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 |
| 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 | started | 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 | | Payments and NFC/SE Manager |
| SENS | started | System Event Notification 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 | started | 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 | started | Windows Modules Installer |
| tzautoupdate | | Auto Time Zone Updater |
| 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 |
| 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 | | Windows Update Medic Service |
| WalletService | | WalletService |
| WarpJITSvc | | WarpJITSvc |
| wbengine | | Block Level Backup Engine Service |
| WbioSrvc | | Windows Biometric Service |
| Wcmsvc | started | Windows Connection Manager |
| wcncsvc | | Windows Connect Now - Config Registrar |
| WdiServiceHost | started | Diagnostic Service Host |
| WdiSystemHost | started | 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 | started | 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 |
| uhssvc | | Microsoft Update Health Service |
| AarSvc_6faaec | | Agent Activation Runtime_6faaec |
| BcastDVRUserService_6faaec | | GameDVR and Broadcast User Service_6faaec |
| BluetoothUserService_6faaec | | Bluetooth User Support Service_6faaec |
| CaptureService_6faaec | | CaptureService_6faaec |
| cbdhsvc_6faaec | started | Clipboard User Service_6faaec |
| CDPUserSvc_6faaec | started | Connected Devices Platform User Service_6faaec |
| ConsentUxUserSvc_6faaec | | ConsentUX_6faaec |
| CredentialEnrollmentManagerUserSvc_6faaec | | CredentialEnrollmentManagerUserSvc_6faaec |
| DeviceAssociationBrokerSvc_6faaec | | DeviceAssociationBroker_6faaec |
| DevicePickerUserSvc_6faaec | | DevicePicker_6faaec |
| DevicesFlowUserSvc_6faaec | | DevicesFlow_6faaec |
| MessagingService_6faaec | | MessagingService_6faaec |
| OneSyncSvc_6faaec | started | Sync Host_6faaec |
| PimIndexMaintenanceSvc_6faaec | | Contact Data_6faaec |
| PrintWorkflowUserSvc_6faaec | | PrintWorkflow_6faaec |
| UdkUserSvc_6faaec | | Udk User Service_6faaec |
| UnistoreSvc_6faaec | | User Data Storage_6faaec |
| UserDataSvc_6faaec | | User Data Access_6faaec |
| WpnUserService_6faaec | started | Windows Push Notifications User Service_6faaec |

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 |
| 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 | | 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 |

| | | |
|---|---|---|
| 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 | started | FAT12/16/32 File System Driver |
| fdc | started | Floppy Disk Controller Driver |
| FileCrypt | started | FileCrypt |
| FileInfo | started | File Information FS MiniFilter |
| Filetrace | | Filetrace |
| flpydisk | started | 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 |
| 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 |
| 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 |
| mrxsmb10 | started | SMB 1.x MiniRedirector |
| 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 |
| 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 | started | Remote Access NDIS TAPI Driver |
| Ndisuio | | NDIS Usermode I/O Protocol |
| NdisVirtualBus | started | Microsoft Virtual Network Adapter Enumerator |
| NdisWan | started | Remote Access NDIS WAN Driver |
| ndiswanlegacy | | Remote Access LEGACY NDIS WAN Driver |
| NDKPing | | NDKPing Driver |
| ndproxy | started | 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 | started | 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 | started | WAN Miniport (IKEv2) |
| Rasl2tp | started | WAN Miniport (L2TP) |
| RasPppoe | started | Remote Access PPPOE Driver |
| RasSstp | started | 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 |
| 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 |

| | | |
|---|---|---|
| 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 |
| Ucx01000 | started | USB Host Support Library |
| UdeCx | | USB Device Emulation Support Library |
| udfs | | udfs |
| UEFI | | Microsoft UEFI Driver |
| Ufx01000 | | USB Function Class Extension |
| UfxChipidea | | USB Chipidea Controller |
| ufxsynopsys | | USB Synopsys Controller |
| umbus | started | UMBus Enumerator Driver |
| UmPass | | 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 |
| 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 | started | 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

## 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 | = | Core |
| InstallationType | = | Client |
| ProductName | = | Windows 10 Home |
| ReleaseId | = | 2009 |
| UBR | = | 2965 |
| DisplayVersion | = | 22H2 |
| HKLM\SYSTEM\currentControlSet\Control\ProductOptions | | |
| ProductType | = | WinNT |
| ProductSuite | = | {"Terminal Server", "Personal"} |

## 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 11.0.19041.1566

 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 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):  2023/12/20 20:46:09

### 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\\vboxuser' | 2023/12/21 05:37:56 |
| 'C:\\Windows\\ServiceProfiles\\NetworkService' | 2023/12/21 05:37:56 |
| 'C:\\Windows\\ServiceProfiles\\LocalService' | 2023/12/21 05:37:56 |
| 'C:\\Windows\\system32\\config\\systemprofile' | 2023/12/21 05:37:56 |

## 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:  Thursday, December 21, 2023 00:00:33 GMT

### 1 List of Microsoft Patches Installed on System

| | |
|---|---|
| QID: | 91328 |
| Category: | Windows |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 04/20/2022 |
| 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
'KB5022502'
'KB5011048'
'KB5015684'
'KB5026361'
'KB5014032'
'KB5025315'
'KB5032907'

### 1 Java Enabled in the Internet Zone

| | |
|---|---|
| QID: | 100141 |
| Category: | Internet Explorer |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 03/13/2013 |
| 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: | 05/10/2005 |
| 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
HKCR\Installer\Products 2C6A1CF1E675A984B9A4292DF1451263
HKCR\Installer\Products A21036B76CA46C046BFA2BA44853D95D

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 69 Stepping 1 |
| ProcessorNameString | = | Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz |
| VendorIdentifier | = | GenuineIntel |
| ~MHz | = | 2607 |

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-bfc1-0800 2be10318}\0000 |
| Dev: | @msmouse.inf, %*pnp0f03.devicedesc%;Microso ft PS/2 Mouse |
| Manufacturer: | @msmouse.inf, %msmfg%;Microsoft |
| Service: | i8042prt |

| | | | | |
|---|---|---|---|---|
| Driver Instance: | {4d36e96f-e325-11ce-bfc1-0800 2be10318}\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-bfc1-0800 2be10318}\0000 | | | |
| Dev: | @keyboard.inf, %*pnp0303.devicedesc%;Standar d | 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: | 07/08/2014 |
| 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_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes
%windir%\system32\regedt32.exe Administrators 544 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\system32\regedt32.exe SYSTEM 18 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\system32\regedt32.exe Users 545 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\system32\regedt32.exe APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES 1 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\system32\regedt32.exe APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES 2 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute

1 File Access Permissions for Regedit.exe

| | |
|---|---|
| QID: | 105154 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 03/26/2005 |
| 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_read append_data delete_child write_attributes read_attributes read_extended_attributes write_data read_data standard_write_owner standard_delete synchronize execute standard_write_dac write_extended_attributes
%windir%\regedit.exe Administrators 544 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\regedit.exe SYSTEM 18 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\regedit.exe Users 545 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\regedit.exe APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES 1 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute
%windir%\regedit.exe APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES 2 access_allowed standard_read read_attributes read_extended_attributes read_data synchronize execute

## 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 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 |
| WIN10\vboxuser | 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 4.18.23110.3
From Local Registry Windows Defender SignaturesLastUpdated Value is:  Thursday, December 21, 2023 05:00:22 GMT
From Local Registry Windows Defender ASSignatureApplied Value is:  Wednesday, December 20, 2023 21:58:54 GMT
From Local Registry Windows Defender AVSignatureApplied Vaule is:  Wednesday, December 20, 2023 21:58:53 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 = 048f08fc9e33da01
InstallLocation = C:\ProgramData\Microsoft\Windows Defender\platform\4.18.23110.3-0\
ManagedDefenderProductType = 0
ProductStatus = 0
OOBEInstallTime = b88f04cba033da01
HybridModeEnabled = 0
VerifiedAndReputableTrustModeEnabled = 0
DisableAntiSpyware = 0
DisableAntiVirus = 0
RpcServerUseEndpointMapper = 0
IsServiceRunning = 1
---
HKLM\SOFTWARE\Microsoft\Windows Defender\CoreService
MdTrustedRootCertThumbPrints =
CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F|4348A0E9444C78CB265E058D5E8944B4D84F9662BD26DB257F8934A443C70161
MdTrustedSubjectOrgs = Microsoft Corporation|DigiCert Inc
WdTimerInitalDelay = 300002
WdTimerMonitorInterval = 300000
WdConfigHash = 1370359201
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Diagnostics
InitializingComponentProgress = ServiceStartedSuccessfully
LatestPlatformVersionOnDevice = 0300465a12000400
LastKnownGoodEngineCandidate = 0200465a01000100
CleanupComponentProgress = CleanupCompleted
PlatformHealthData =
0300000030010000000000000000000000000000000000000400000000000000000000000000000000000000000000000400000000000000000000000000000000000000000000000000000003000000
0000000000000000000000000000000000000003000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000002000000000000
0000000000000000000000000000000002000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000002000000000000000000
0000000000000000000000030000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000100000000000000
LastSignatureUpdateResult = 0
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Features
TamperProtection = 1
MpPlatformKillbitsFromEngine = 0000000400000000
TPExclusions = 0
MpPlatformKillbitsExFromEngine =
2000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
TamperProtectionSource = 5
EnableCACS = 0
MpCapability = ff01000000000000
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Miscellaneous Configuration
DeltaUpdateFailure = 0
BddUpdateFailure = 0
---
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 = dfdd8a8a9f33da01

SigUpdateTimestampsSinceLastHB =
LastRebootTime = 894a66adc833da01
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Scan
EEC13D5D-0000-0000-0000-100000000000 = C:\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\EEC13D5D-0000-0000-0000-100000000000-0.bin
SFCState = 128
DaysUntilAggressiveCatchupQuickScan = 30
AggressiveCatchupQuickScanReattemptElapsed = 23
CacheFile = C:\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\EEC13D5D-0000-0000-0000-100000000000-0.bin
---
HKLM\SOFTWARE\Microsoft\Windows Defender\Signature Updates
DisableDefaultSigs = 0
SignatureCategoryID = 8c3fcc84-7410-4a95-8b89-a166a0190486
EngineVersion = 1.1.23110.2
AVSignatureVersion = 1.403.852.0
AVSignatureBaseVersion = 1.403.0.0
AVSignatureApplied = 804c86b88f33da01
ASSignatureVersion = 1.403.852.0
ASSignatureBaseVersion = 1.403.0.0
ASSignatureApplied = 00e31eb98f33da01
SignatureLocation = C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{712829DF-EDEF-4918-BF78-25946AEFB03D}
SignatureType = 0
SignatureUpdateCount = 2
SignaturesLastUpdated = f409019aca33da01
SignatureUpdatePending = 0
LastFallbackTime = 3b6f713bca33da01
MoCAMPUpdateStarted = 45726c91c733da01
EnableUpdateResiliency = 0
SignatureUpdateLastAttempted = 0a87463bca33da01
---
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/submitReport,REST:https://wdcpalt.microsoft.com/wdcp.svc/submitReport,BOND:https://wdcp.microsoft.com/wdcp.svc/bond/submitreport,BOND:https://wdcpalt.microsoft.com/wdcp.svc/bond/submitreport
SSLOptions = 3
MAPSconcurrency = 1
MAPSconcurrencyDss = 10
LastMAPSSuccessTime = fe539eb1ab33da01
LastMAPSFailureTime = 7dab7aabae33da01
---
Malware Protection Engine Version:
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{712829DF-EDEF-4918-BF78-25946AEFB03D}\mpengine.dll Version is 1.1.23110.2

 1 Microsoft System Center Configuration Manager Client (SCCM) Not Installed

| | |
|---|---|
| QID: | 105504 |
| Category: | Security Policy |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 04/01/2014 |
| 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: 555253981184 582368620544
D: 0 53448704

### 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 : 4294496256

## 1 Microsoft Windows Malicious Software Removal Tool Detected

| | |
|---|---|
| QID: | 121213 |
| Category: | Local |
| Associated CVEs: | - |
| Vendor Reference: | Malware Removal Tool |
| Bugtraq ID: | - |
| Service Modified: | 06/03/2013 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |

THREAT:

Microsoft Windows Malicious Software Removal Tool is a malware removal tool.
The program is automatically distributed to Microsoft Windows computers via Windows Update service but can also be separately downloaded. (http://www.microsoft.com/security/pc-security/malware-removal.aspx)
Malware Removal Tool was detected on 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:

HKLM\SOFTWARE\Microsoft\RemovalTools\MRT Version = ABE6CED3-EAE8-4BBB-AE10-FB3F05CA9020

## 1 Windows Forensics MRU Enumeration - Regedit.exe

| | |
|---|---|
| QID: | 125017 |
| Category: | Forensics |
| Associated CVEs: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 09/16/2014 |
| 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: | WIN10\vboxuser | VAL: | Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System |

# Appendix

## Hosts Scanned (IP)

192.168.0.4

## Target distribution across scanner appliances

kdee : 192.168.0.4

## Windows authentication was successful for these hosts (1)

Instance os:
192.168.0.4

## Options Profile

## basicnetscan

### 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 |
| 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. |
| 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 |

| Severity | Level | Description |
|---|---|---|
| | | 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. |