Scan Report

July 25, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Scan-Azure-Win10Vulnerable -Credentialed". The scan started at Tue Jul 25 03:45:37 2023 UTC and ended at Tue Jul 25 04:06:35 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.5 windows10-vulne	62	21	1	0	0
Total: 1	62	21	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 84 results selected by the filtering described above. Before filtering there were 144 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.5 - windows10-vulne	SMB	Success	Protocol SMB, Port 445, User cybersuhanlab

2 Results per Host

2.1 10.0.0.5

Host scan start	Tue Jul 25 03:46:17 2023 UTC
Host scan end	Tue Jul 25 04:06:27 2023 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium
135/tcp	Medium
3389/tcp	Medium
general/icmp	Low

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa_2022-54_2023-02)-Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 97.0`
`Fixed version: 109`
`Installation path / port: C:\Program Files\Mozilla Firefox`

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause denial of service, disclose sensitive information and conduct spoofing attack.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 109 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 109 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Logic bug in process allocation allowed to read arbitrary files.
- Malicious command could be hidden in devtools output on Windows.
- URL being dragged from cross-origin iframe into same tab triggers navigation.
- Content Security Policy wasn't being correctly applied to WebSockets in WebWorkers.
- Calls to <code>console.log</code> allowed bypassing Content Security Policy via format directive.
- Creation of duplicate <code>SystemPrincipal</code> from less secure contexts.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update(mfsa_2022-54_2023-02)-Windows`
OID:1.3.6.1.4.1.25623.1.0.826789
Version used: `2023-01-19T10:10:48Z`

References
`cve: CVE-2023-23597`
`cve: CVE-2023-23598`
`cve: CVE-2023-23599`
`cve: CVE-2023-23601`
`cve: CVE-2023-23602`
`cve: CVE-2023-23603`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2023-23604
cve: CVE-2023-23605
cve: CVE-2023-23606
url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0107
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0408
dfn-cert: DFN-CERT-2023-0146
dfn-cert: DFN-CERT-2023-0104

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities - 01 Jan14 (Windows)

Summary
Adobe Reader is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will allow attackers to, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Update to Adobe Reader Version 10.1.9 or 11.0.06 or later.

Affected Software/OS
Adobe Reader X Version 10.x prior to 10.1.9 on Windows
Adobe Reader XI Version 11.x prior to 11.0.06 on Windows

Vulnerability Insight
Flaw is due to some unspecified errors and an error in dereferencing already freed memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader Multiple Vulnerabilities - 01 Jan14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804068
Version used: 2022-08-09T10:11:17Z

References
cve: CVE-2014-0493
cve: CVE-2014-0495
cve: CVE-2014-0496

... continues on next page ...

... continued from previous page ...

```
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://secunia.com/advisories/56303
url: http://www.securityfocus.com/bid/64802
url: http://www.securityfocus.com/bid/64803
url: http://www.securityfocus.com/bid/64804
url: http://helpx.adobe.com/security/products/acrobat/apsb14-01.html
cert-bund: CB-K14/0045
dfn-cert: DFN-CERT-2014-0044
```

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities - 01 July15 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 10.0.0`
`Fixed version: 10.1.15`

Impact
Successful exploitation will allow attackers to conduct a denial of service, bypass certain security restrictions, to obtain sensitive information, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.15 or 11.0.12 or later.

Affected Software/OS
Adobe Reader 10.x before 10.1.15 and 11.x before 11.0.12 on Windows.

Vulnerability Insight
Multiple flaws are due to:
- Multiple memory corruption vulnerabilities.
- Multiple use-after-free vulnerabilities.
- Multiple integer over flow vulnerabilities.
- Multiple buffer over flow vulnerabilities.
- Some unspecified vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Vulnerabilities - 01 July15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805679
Version used: `2022-04-14T06:42:08Z`

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2015-5115
cve: CVE-2015-5114
cve: CVE-2015-5113
cve: CVE-2015-5111
cve: CVE-2015-5110
cve: CVE-2015-5109
cve: CVE-2015-5108
cve: CVE-2015-5107
cve: CVE-2015-5106
cve: CVE-2015-5105
cve: CVE-2015-5104
cve: CVE-2015-5103
cve: CVE-2015-5102
cve: CVE-2015-5101
cve: CVE-2015-5100
cve: CVE-2015-5099
cve: CVE-2015-5098
cve: CVE-2015-5097
cve: CVE-2015-5096
cve: CVE-2015-5095
cve: CVE-2015-5094
cve: CVE-2015-5093
cve: CVE-2015-5092
cve: CVE-2015-5091
cve: CVE-2015-5090
cve: CVE-2015-5089
cve: CVE-2015-5088
cve: CVE-2015-5087
cve: CVE-2015-5086
cve: CVE-2015-5085
cve: CVE-2015-4452
cve: CVE-2015-4451
cve: CVE-2015-4450
cve: CVE-2015-4449
cve: CVE-2015-4448
cve: CVE-2015-4447
cve: CVE-2015-4446
cve: CVE-2015-4445
cve: CVE-2015-4444
cve: CVE-2015-4443
cve: CVE-2015-4441
cve: CVE-2015-4438
cve: CVE-2015-4435
cve: CVE-2015-3095
cve: CVE-2014-8450

... continues on next page ...

... continued from previous page ...

cve: CVE-2014-0566
url: http://www.securityfocus.com/bid/75740
url: http://www.securityfocus.com/bid/75739
url: http://www.securityfocus.com/bid/75746
url: http://www.securityfocus.com/bid/75741
url: http://www.securityfocus.com/bid/75747
url: http://www.securityfocus.com/bid/69825
url: http://www.securityfocus.com/bid/75748
url: http://www.securityfocus.com/bid/75742
url: http://www.securityfocus.com/bid/75738
url: http://www.securityfocus.com/bid/75743
url: http://www.securityfocus.com/bid/75737
url: http://www.securityfocus.com/bid/75735
url: http://www.securityfocus.com/bid/75749
url: http://www.securityfocus.com/bid/75402
url: https://helpx.adobe.com/security/products/acrobat/apsb15-15.html
cert-bund: CB-K15/1002
cert-bund: CB-K14/1163
dfn-cert: DFN-CERT-2015-1053
dfn-cert: DFN-CERT-2014-1224

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities - 01 May14 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will allow attackers to conduct a denial of service, disclose potentially sensitive information, bypass certain security restrictions, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader X version 10.1.10 or XI version 11.0.07 or later.

Affected Software/OS
Adobe Reader X before version 10.1.10 and XI before version 11.0.07 on Windows.

Vulnerability Insight
Multiple flaws exist:
- An error within the implementation of Javascript APIs.
- An error when validating user supplied paths.

... continues on next page ...

... continued from previous page ...

- An integer overflow error when handling PDF417 barcodes.
- An error exists within the handling of certain API calls to unmapped memory.
- A use-after-free error when handling the messageHandler property of the AcroPDF ActiveX control.
- A double-free error.
- Many other unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Vulnerabilities - 01 May14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804606
Version used: `2022-04-14T11:24:11Z`

References
`cve: CVE-2014-0521`
`cve: CVE-2014-0522`
`cve: CVE-2014-0523`
`cve: CVE-2014-0524`
`cve: CVE-2014-0525`
`cve: CVE-2014-0526`
`cve: CVE-2014-0527`
`cve: CVE-2014-0528`
`cve: CVE-2014-0529`
`url: http://securitytracker.com/id/1030229`
`url: http://www.securityfocus.com/bid/67360`
`url: http://www.securityfocus.com/bid/67362`
`url: http://www.securityfocus.com/bid/67363`
`url: http://www.securityfocus.com/bid/67365`
`url: http://www.securityfocus.com/bid/67366`
`url: http://www.securityfocus.com/bid/67367`
`url: http://www.securityfocus.com/bid/67368`
`url: http://www.securityfocus.com/bid/67369`
`url: http://www.securityfocus.com/bid/67370`
`url: https://www.hkcert.org/my_url/en/alert/14051403`
`url: http://helpx.adobe.com/security/products/reader/apsb14-15.html`
`cert-bund: CB-K14/0570`
`dfn-cert: DFN-CERT-2014-0593`

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities - 01 May15 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 10.0.0`

... continues on next page ...

... continued from previous page ...

Fixed version: 10.1.14

Impact
Successful exploitation will allow attackers to conduct a denial of service, bypass certain security restrictions, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.14 or 11.0.11 or later.

Affected Software/OS
Adobe Reader 10.x before 10.1.14 and 11.x before 11.0.11 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- Error 'ScriptBridgeUtils', 'AFParseDate', 'ADBCAnnotEnumerator' 'WDAnnotEnumerator', 'AFNSimple_Calculate', and 'app.Monitors'.
- Multiple user-supplied inputs are not properly validated, and an use-after-free error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader Multiple Vulnerabilities - 01 May15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805383
Version used: 2022-04-14T06:42:08Z

References
cve: CVE-2015-3076
cve: CVE-2015-3075
cve: CVE-2015-3074
cve: CVE-2015-3073
cve: CVE-2015-3072
cve: CVE-2015-3071
cve: CVE-2015-3070
cve: CVE-2015-3069
cve: CVE-2015-3068
cve: CVE-2015-3067
cve: CVE-2015-3066
cve: CVE-2015-3065
cve: CVE-2015-3064
cve: CVE-2015-3063
cve: CVE-2015-3062
cve: CVE-2015-3061
cve: CVE-2015-3060
cve: CVE-2015-3059
cve: CVE-2015-3058
cve: CVE-2015-3057

... continues on next page ...

... continued from previous page ...

cve: CVE-2015-3056
cve: CVE-2015-3055
cve: CVE-2015-3054
cve: CVE-2015-3053
cve: CVE-2015-3052
cve: CVE-2015-3051
cve: CVE-2015-3050
cve: CVE-2015-3049
cve: CVE-2015-3048
cve: CVE-2015-3046
cve: CVE-2015-3047
cve: CVE-2014-9160
url: https://helpx.adobe.com/security/products/reader/apsb15-10.html
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74602
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74604
url: http://www.securityfocus.com/bid/74602
url: http://www.securityfocus.com/bid/74618
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74602
url: http://www.securityfocus.com/bid/74602
url: http://www.securityfocus.com/bid/74602
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74603
url: http://www.securityfocus.com/bid/74600
url: http://www.securityfocus.com/bid/74601
url: http://www.securityfocus.com/bid/74599
cert-bund: CB-K15/0652
dfn-cert: DFN-CERT-2015-0680

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities - Windows

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 10.0.0`
`Fixed version: 9.5.2/10.1.4`
`Installation path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\`

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the affected application or cause a denial of service.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 9.5.2 or 10.1.4 or later.

Affected Software/OS
Adobe Reader versions 9.x through 9.5.1 and 10.x through 10.1.3 on Windows

Vulnerability Insight
The flaws are due to unspecified errors which can be exploited to corrupt memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.802936
Version used: `2022-04-27T12:01:52Z`

References
`cve: CVE-2012-4149`
`cve: CVE-2012-4148`
`cve: CVE-2012-4147`
`cve: CVE-2012-2051`
`cve: CVE-2012-2050`
`cve: CVE-2012-4160`
`cve: CVE-2012-2049`
`cve: CVE-2012-4159`
`cve: CVE-2012-4158`
`cve: CVE-2012-4157`
`cve: CVE-2012-4156`
`cve: CVE-2012-4155`
`cve: CVE-2012-4154`
`cve: CVE-2012-4153`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2012-1525
cve: CVE-2012-4152
cve: CVE-2012-4151
cve: CVE-2012-4150
url: http://secunia.com/advisories/50281
url: http://www.securityfocus.com/bid/55005
url: http://www.securityfocus.com/bid/55006
url: http://www.securityfocus.com/bid/55007
url: http://www.securityfocus.com/bid/55008
url: http://www.securityfocus.com/bid/55010
url: http://www.securityfocus.com/bid/55011
url: http://www.securityfocus.com/bid/55012
url: http://www.securityfocus.com/bid/55013
url: http://www.securityfocus.com/bid/55015
url: http://www.securityfocus.com/bid/55016
url: http://www.securityfocus.com/bid/55017
url: http://www.securityfocus.com/bid/55018
url: http://www.securityfocus.com/bid/55019
url: http://www.securityfocus.com/bid/55020
url: http://www.securityfocus.com/bid/55021
url: http://www.securityfocus.com/bid/55024
url: http://www.securityfocus.com/bid/55026
url: http://www.securityfocus.com/bid/55027
url: http://www.adobe.com/support/security/bulletins/apsb12-16.html
dfn-cert: DFN-CERT-2012-1579

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities April-2012 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will let attackers to bypass certain security restrictions, execute arbitrary code via unspecified vectors or cause a denial of service.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 9.5.1 or 10.1.3 or later.

Affected Software/OS
Adobe Reader version 9.x to 9.5 and prior and 10.x to 10.1.2 on Windows

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaws are due to
- An unspecified error when handling JavaScript/JavaScript API can be exploited to corrupt memory.
- An integer overflow error when handling True Type Font (TTF) can be exploited to corrupt memory.
- The application loads executables (msiexec.exe) in an insecure manner.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Vulnerabilities April-2012 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.802748
Version used: `2022-04-27T12:01:52Z`

References
`cve: CVE-2012-0776`
`cve: CVE-2012-0774`
`cve: CVE-2012-0775`
`url: http://secunia.com/advisories/48733`
`url: http://www.securityfocus.com/bid/52949`
`url: http://www.securityfocus.com/bid/52951`
`url: http://www.securityfocus.com/bid/52952`
`url: http://www.securitytracker.com/id/1026908`
`url: http://www.adobe.com/support/security/bulletins/apsb12-08.html`
`dfn-cert: DFN-CERT-2012-0747`
`dfn-cert: DFN-CERT-2012-0728`
`dfn-cert: DFN-CERT-2012-0662`
`dfn-cert: DFN-CERT-2012-0661`

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities-01 Dec14 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.13 or 11.0.10 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Adobe Reader 10.x before 10.1.13 and Adobe Reader 11.x before 11.0.10 on on Windows.

Vulnerability Insight
Multiple flaws are due to:
- Multiple use-after-free errors can be exploited to execute arbitrary code.
- Multiple unspecified errors can be exploited to cause a heap-based buffer overflow and subsequently execute arbitrary code.
- A Race condition in the MoveFileEx call hook feature allows attackers to bypass a sandbox protection mechanism.
- An error within the implementation of a Javascript API can be exploited to disclose certain information.
- Multiple integer overflow errors can be exploited to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Vulnerabilities-01 Dec14 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.805303
Version used: `2022-04-14T11:24:11Z`

References
`cve: CVE-2014-9150`
`cve: CVE-2014-9165`
`cve: CVE-2014-8445`
`cve: CVE-2014-8446`
`cve: CVE-2014-8447`
`cve: CVE-2014-8448`
`cve: CVE-2014-8449`
`cve: CVE-2014-8451`
`cve: CVE-2014-8452`
`cve: CVE-2014-8453`
`cve: CVE-2014-8454`
`cve: CVE-2014-8455`
`cve: CVE-2014-8456`
`cve: CVE-2014-8457`
`cve: CVE-2014-8458`
`cve: CVE-2014-8459`
`cve: CVE-2014-8461`
`cve: CVE-2014-9158`
`cve: CVE-2014-9159`
`cve: CVE-2014-8460`
`url: http://secunia.com/advisories/61095/`
`url: http://www.securityfocus.com/bid/71366`
`url: http://www.securityfocus.com/bid/71557`
`url: http://www.securityfocus.com/bid/71561`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/71562
url: http://www.securityfocus.com/bid/71564
url: http://www.securityfocus.com/bid/71565
url: http://www.securityfocus.com/bid/71566
url: http://www.securityfocus.com/bid/71567
url: http://www.securityfocus.com/bid/71568
url: http://www.securityfocus.com/bid/71570
url: http://www.securityfocus.com/bid/71571
url: http://www.securityfocus.com/bid/71572
url: http://www.securityfocus.com/bid/71573
url: http://www.securityfocus.com/bid/71574
url: http://www.securityfocus.com/bid/71575
url: http://www.securityfocus.com/bid/71576
url: http://www.securityfocus.com/bid/71577
url: http://www.securityfocus.com/bid/71578
url: http://www.securityfocus.com/bid/71579
url: http://www.securityfocus.com/bid/71580
url: http://helpx.adobe.com/security/products/reader/apsb14-28.html
url: https://code.google.com/p/google-security-research/issues/detail?id=103
cert-bund: CB-K15/0652
cert-bund: CB-K14/1527
dfn-cert: DFN-CERT-2015-0680
dfn-cert: DFN-CERT-2014-1624
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa_2023-04_2023-06)-Windows

Summary
Mozilla Firefox and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 97.0
Fixed version:     110
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact
Successful exploitation will allow attackers to execute arbitrary code, disclose sensitive information and conduct spoofing attacks.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 110 or later, Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Mozilla Firefox version before 110 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Content security policy leak in violation reports using iframes.
- Screen hijack via browser fullscreen mode.
- Arbitrary memory write via PKCS 12 in NSS.
- Potential use-after-free from compartment mismatch in SpiderMonkey.
- Invalid downcast in SVGUtils::SetupStrokeGeometry.
- Printing on Windows could potentially crash Firefox with some device drivers.
- Use-after-free in mozilla::dom::ScriptLoadContext:: ScriptLoadContext.
- Extensions could have opened external schemes without user knowledge.
- Out of bounds memory write from EncodeInputStream.
- Opening local .url files could cause unexpected network loads.
- Web Crypto ImportKey crashes tab.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa_2023-04_2023-06)-Windows`
OID:1.3.6.1.4.1.25623.1.0.832011
Version used: `2023-03-06T10:19:58Z`

References
`cve: CVE-2023-25728`
`cve: CVE-2023-25730`
`cve: CVE-2023-0767`
`cve: CVE-2023-25745`
`cve: CVE-2023-25735`
`cve: CVE-2023-25737`
`cve: CVE-2023-25738`
`cve: CVE-2023-25739`
`cve: CVE-2023-25729`
`cve: CVE-2023-25732`
`cve: CVE-2023-25734`
`cve: CVE-2023-25740`
`cve: CVE-2023-25731`
`cve: CVE-2023-25733`
`cve: CVE-2023-25736`
`cve: CVE-2023-25741`
`cve: CVE-2023-25742`
`cve: CVE-2023-25744`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0407`
`cert-bund: WID-SEC-2023-0385`
`dfn-cert: DFN-CERT-2023-1243`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0843
dfn-cert: DFN-CERT-2023-0411
dfn-cert: DFN-CERT-2023-0408
dfn-cert: DFN-CERT-2023-0395
dfn-cert: DFN-CERT-2023-0394
dfn-cert: DFN-CERT-2023-0340

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Vulnerabilities-01 Sep14 (Windows)

Summary
Adobe Reader is prone to multiple vulnerabilities.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, execute arbitrary code and compromise a user's system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.12 or 11.0.09 or later.

Affected Software/OS
Adobe Reader 10.x before 10.1.12 and 11.x before 11.0.09 on Windows.

Vulnerability Insight
Multiple flaws are due to:
- An use-after-free error can be exploited to execute arbitrary code.
- An error within the implementation of the 'replace()' JavaScript function can be exploited to cause a heap-based buffer overflow via specially crafted arguments.
- An error within the 3DIF Plugin (3difr.x3d) can be exploited to cause a heap-based buffer overflow via a specially crafted PDF file.
- Some unspecified errors can be exploited to cause a memory corruption.
- An unspecified error can be exploited to bypass certain sandbox restrictions.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader Multiple Vulnerabilities-01 Sep14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804485
Version used: 2022-04-14T11:24:11Z

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2014-0560
cve: CVE-2014-0561
cve: CVE-2014-0563
cve: CVE-2014-0565
cve: CVE-2014-0566
cve: CVE-2014-0567
cve: CVE-2014-0568
url: http://secunia.com/advisories/60901
url: http://www.securityfocus.com/bid/69821
url: http://www.securityfocus.com/bid/69823
url: http://www.securityfocus.com/bid/69824
url: http://www.securityfocus.com/bid/69825
url: http://www.securityfocus.com/bid/69826
url: http://www.securityfocus.com/bid/69827
url: http://www.securityfocus.com/bid/69828
url: http://helpx.adobe.com/security/products/reader/apsb14-20.html
cert-bund: CB-K15/1002
cert-bund: CB-K14/1163
dfn-cert: DFN-CERT-2015-1053
dfn-cert: DFN-CERT-2014-1224

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa2022-24) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 102
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 102 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 102 on Windows.

Vulnerability Insight
Multiple flaws exist due to,

... continues on next page ...

... continued from previous page ...

- A popup window could be resized in a way to overlay the address bar with web content.
- Use-after-free in nsSHistory.
- CSP sandbox header without 'allow-scripts' can be bypassed via retargeted javascript: URI.
- Drag and drop of malicious image could have led to malicious executable and potential code execution.
- ASN.1 parser could have been tricked into accepting malformed ASN.1.
- Potential integer overflow in ReplaceElementsAt.
- Sandboxed iframes could redirect to external schemes.
- TLS certificate errors on HSTS-protected domains could be bypassed by the user on Firefox for Android.
- Compromised server could trick a browser into an addon downgrade.
- Unavailable PAC file resulted in OCSP requests being blocked.
- Microsoft protocols can be attacked if a user accepts a prompt.
- Undesired attributes could be set as part of prototype pollution.
- Free of uninitialized pointer in lg_init.
- MediaError message property leaked information on cross-origin same-site pages.
- HTML Sanitizer could have been bypassed via same-origin script via use tags.
- HTML Sanitizer could have been bypassed via use tags.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa2022-24) - Windows`
OID:1.3.6.1.4.1.25623.1.0.821169
Version used: `2022-07-14T10:10:42Z`

References
`cve: CVE-2022-34470`
`cve: CVE-2022-34468`
`cve: CVE-2022-34482`
`cve: CVE-2022-34483`
`cve: CVE-2022-34476`
`cve: CVE-2022-34481`
`cve: CVE-2022-34474`
`cve: CVE-2022-34471`
`cve: CVE-2022-34472`
`cve: CVE-2022-34478`
`cve: CVE-2022-2200`
`cve: CVE-2022-34480`
`cve: CVE-2022-34477`
`cve: CVE-2022-34475`
`cve: CVE-2022-34473`
`cve: CVE-2022-34484`
`cve: CVE-2022-34485`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-24`
`cert-bund: WID-SEC-2022-1251`
`cert-bund: WID-SEC-2022-0505`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1535
dfn-cert: DFN-CERT-2022-1524
dfn-cert: DFN-CERT-2022-1441
dfn-cert: DFN-CERT-2022-1440

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa2022-20) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 101
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 101 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 101 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Cross-Origin resource's length leaked.
- Heap buffer overflow in WebGL.
- Browser window spoof using fullscreen mode.
- Attacker-influenced path traversal when saving downloaded files.
- Register allocation problem in WASM on arm64.
- Uninitialized variable leads to invalid memory read.
- Querying a WebAuthn token with a large number of allowCredential entries may have leaked cross-origin information.
- HTML Parsing incorrectly ended HTML comments prematurely.
- CSP bypass enabling stylesheet injection.
- Incorrect Assertion caused by unoptimized array shift operations.
- Memory Corruption when manipulating webp images.

... continues on next page ...

... continued from previous page ...

- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates(mfsa2022-20) - Windows
OID:1.3.6.1.4.1.25623.1.0.821167
Version used: 2022-07-14T10:10:42Z

References
cve: CVE-2022-31736
cve: CVE-2022-31737
cve: CVE-2022-31738
cve: CVE-2022-31739
cve: CVE-2022-31740
cve: CVE-2022-31741
cve: CVE-2022-31742
cve: CVE-2022-31743
cve: CVE-2022-31744
cve: CVE-2022-31745
cve: CVE-2022-1919
cve: CVE-2022-31747
cve: CVE-2022-31748
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-20
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0019
cert-bund: CB-K22/0671
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1535
dfn-cert: DFN-CERT-2022-1441
dfn-cert: DFN-CERT-2022-1440
dfn-cert: DFN-CERT-2022-1430
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1303
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1231
dfn-cert: DFN-CERT-2022-1230

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa2022-19) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 100.0.2
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, escalate privileges on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 100.0.2 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 100.0.2 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Prototype pollution in Top-Level Await implementation.
- Untrusted input used in JavaScript object indexing, leading to prototype pollution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates(mfsa2022-19) - Windows
OID:1.3.6.1.4.1.25623.1.0.821165
Version used: 2022-07-14T10:10:42Z

References
cve: CVE-2022-1802
cve: CVE-2022-1529
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-19
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-0129
cert-bund: CB-K22/0642
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
dfn-cert: DFN-CERT-2022-1162

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa2022-16) - Windows

Summary

... continues on next page ...

... continued from previous page ...

Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 97.0
Fixed version:     100
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact

Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:

Solution type: VendorFix

Upgrade to Mozilla Firefox version 100 or later, Please see the references for more information.

Affected Software/OS

Mozilla Firefox version before 100 on Windows.

Vulnerability Insight

Multiple flaws exist due to,
- Fullscreen notification bypass using popups.
- Bypassing permission prompt in nested browsing contexts.
- Leaking browser history with CSS variables.
- iframe Sandbox bypass.
- Reader mode bypassed SameSite cookies.
- Firefox for Android forgot HTTP Strict Transport Security settings.
- Leaking cross-origin redirect through the Performance API.
- Memory safety bugs.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Mozilla Firefox Security Updates(mfsa2022-16) - Windows`

OID:1.3.6.1.4.1.25623.1.0.821163

Version used: `2022-07-14T10:10:42Z`

References

```
cve: CVE-2022-29914
cve: CVE-2022-29909
cve: CVE-2022-29916
cve: CVE-2022-29911
cve: CVE-2022-29912
cve: CVE-2022-29915
cve: CVE-2022-29917
cve: CVE-2022-29918
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-16
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0538
cert-bund: WID-SEC-2022-0537
cert-bund: CB-K22/0542
cert-bund: CB-K22/0534
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
dfn-cert: DFN-CERT-2022-1007
dfn-cert: DFN-CERT-2022-1003
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0978

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa2022-10) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 98
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 98 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 98 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Browser window spoof using fullscreen mode.
- iframe allow-scripts sandbox bypass.
- Time-of-check time-of-use bug when verifying add-on signatures.
- Use-after-free in text reflows.
- Autofill Text could be exfiltrated via side-channel attacks.
- Use-after-free in thread shutdown.

... continues on next page ...

... continued from previous page ...

- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates(mfsa2022-10) - Windows
OID:1.3.6.1.4.1.25623.1.0.821159
Version used: 2022-07-14T10:10:42Z

References
cve: CVE-2022-26383
cve: CVE-2022-26384
cve: CVE-2022-26387
cve: CVE-2022-26381
cve: CVE-2022-26382
cve: CVE-2022-26385
cve: CVE-2022-0843
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-10
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1034
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0283
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0688
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0551
dfn-cert: DFN-CERT-2022-0516

High (CVSS: 10.0)
NVT: Adobe Reader End Of Life Detection (Windows)

Summary
The Adobe Reader version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "Adobe Reader" version on the remote host has reached the end of life.
CPE: cpe:/a:adobe:acrobat_reader:10.0.0
Installed version: 10.0.0
EOL version: 10
EOL date: 2015-11-18

... continues on next page ...

... continued from previous page ...

Impact
An end of life version of Adobe Reader is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update the Adobe Reader version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an unsupported version is present on the target host.
Details: `Adobe Reader End Of Life Detection (Windows)`
OID:1.3.6.1.4.1.25623.1.0.814035
Version used: `2023-07-20T05:05:17Z`

References
`url: https://helpx.adobe.com/support/programs/eol-matrix.html`

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Unspecified Vulnerabilities -01 May13 (Windows)

Summary
Adobe Reader is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow attacker to execute arbitrary code, corrupt memory, obtain sensitive information, bypass certain security restrictions or cause a denial of service condition.

Solution:
Solution type: VendorFix
Update to Adobe Reader Version 11.0.03 or 10.1.7 or 9.5.5 or later.

Affected Software/OS
Adobe Reader Version 9.x prior to 9.5.5 on Windows
Adobe Reader X Version 10.x prior to 10.1.7 on Windows
Adobe Reader XI Version 11.x prior to 11.0.03 on Windows

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Adobe Reader Multiple Unspecified Vulnerabilities -01 May13 (Windows)

OID:1.3.6.1.4.1.25623.1.0.803613

Version used: 2022-08-09T10:11:17Z

References

cve: CVE-2013-3342
cve: CVE-2013-3341
cve: CVE-2013-3340
cve: CVE-2013-3339
cve: CVE-2013-3338
cve: CVE-2013-3337
cve: CVE-2013-2737
cve: CVE-2013-2736
cve: CVE-2013-2735
cve: CVE-2013-2734
cve: CVE-2013-2733
cve: CVE-2013-2732
cve: CVE-2013-2731
cve: CVE-2013-2730
cve: CVE-2013-2729
cve: CVE-2013-2727
cve: CVE-2013-2726
cve: CVE-2013-2725
cve: CVE-2013-2724
cve: CVE-2013-2723
cve: CVE-2013-2722
cve: CVE-2013-2721
cve: CVE-2013-2720
cve: CVE-2013-2719
cve: CVE-2013-2718
cve: CVE-2013-3346
cve: CVE-2013-2549
cve: CVE-2013-2550
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://secunia.com/advisories/53420
url: http://www.securityfocus.com/bid/58398
url: http://www.securityfocus.com/bid/58568
url: http://www.securityfocus.com/bid/59902
url: http://www.securityfocus.com/bid/59903
url: http://www.securityfocus.com/bid/59904
url: http://www.securityfocus.com/bid/59905
url: http://www.securityfocus.com/bid/59906
url: http://www.securityfocus.com/bid/59907
url: http://www.securityfocus.com/bid/59908

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/59909
url: http://www.securityfocus.com/bid/59910
url: http://www.securityfocus.com/bid/59911
url: http://www.securityfocus.com/bid/59912
url: http://www.securityfocus.com/bid/59913
url: http://www.securityfocus.com/bid/59914
url: http://www.securityfocus.com/bid/59915
url: http://www.securityfocus.com/bid/59916
url: http://www.securityfocus.com/bid/59917
url: http://www.securityfocus.com/bid/59918
url: http://www.securityfocus.com/bid/59919
url: http://www.securityfocus.com/bid/59920
url: http://www.securityfocus.com/bid/59921
url: http://www.securityfocus.com/bid/59923
url: http://www.securityfocus.com/bid/59925
url: http://www.securityfocus.com/bid/59926
url: http://www.securityfocus.com/bid/59927
url: http://www.securityfocus.com/bid/59930
url: http://www.adobe.com/support/security/bulletins/apsb13-15.html
dfn-cert: DFN-CERT-2013-1065
dfn-cert: DFN-CERT-2013-0929
dfn-cert: DFN-CERT-2013-0908
dfn-cert: DFN-CERT-2013-0905

High (CVSS: 10.0)
NVT: Adobe Reader Multiple Unspecified Vulnerabilities-01 Sep13 (Windows)

Summary
Adobe Reader is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
Successful exploitation will allow attacker to execute arbitrary code, cause a denial of service condition and potentially allow to take control of the affected system.

Solution:
Solution type: VendorFix
Update to Adobe Reader Version 11.0.04 or 10.1.8 or later.

Affected Software/OS
Adobe Reader X Version 10.x prior to 10.1.8 on Windows
Adobe Reader XI Version 11.x prior to 11.0.04 on Windows

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to:
- An integer overflow error when handling U3D PCX external texture.
- Other multiple unspecified and integer overflow errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Unspecified Vulnerabilities-01 Sep13 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803893
Version used: `2022-04-25T14:50:49Z`

References
`cve: CVE-2013-3351`
`cve: CVE-2013-3352`
`cve: CVE-2013-3353`
`cve: CVE-2013-3354`
`cve: CVE-2013-3355`
`cve: CVE-2013-3356`
`cve: CVE-2013-3357`
`cve: CVE-2013-3358`
`url: http://secunia.com/advisories/54694`
`url: http://www.securityfocus.com/bid/62428`
`url: http://www.securityfocus.com/bid/62429`
`url: http://www.securityfocus.com/bid/62430`
`url: http://www.securityfocus.com/bid/62431`
`url: http://www.securityfocus.com/bid/62432`
`url: http://www.securityfocus.com/bid/62433`
`url: http://www.securityfocus.com/bid/62435`
`url: http://www.securityfocus.com/bid/62436`
`url: https://www.adobe.com/support/security/bulletins/apsb13-22.html`
`cert-bund: CB-K13/0642`
`dfn-cert: DFN-CERT-2013-1624`

High (CVSS: 10.0)
NVT: Adobe Reader Sandbox Bypass Vulnerability (Aug 2014) - Windows

Summary
Adobe Reader is prone to a sandbox bypass vulnerability.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow attacker to bypass sandbox restrictions and execute native code in a privileged context.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to version 10.1.11 or 11.0.08 or later.

Affected Software/OS
Adobe Reader X version 10.x before 10.1.11 and XI version 11.x before 11.0.08 on Windows.

Vulnerability Insight
Flaw exists due to some unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Sandbox Bypass Vulnerability (Aug 2014) - Windows`
OID:1.3.6.1.4.1.25623.1.0.804813
Version used: `2022-08-09T10:11:17Z`

References
`cve: CVE-2014-0546`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: http://helpx.adobe.com/security/products/reader/apsb14-19.html`
`url: http://www.securityfocus.com/bid/69193`
`cert-bund: CB-K14/1001`
`dfn-cert: DFN-CERT-2014-1048`

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates (mfsa_2023-22_2023-24) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 97.0
Fixed version:     115
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact
Successful exploitation allow attackers to disclose sensitive information, execute arbitrary code and cause denial of service condition on an affected system.

Solution:
Solution type: VendorFix
Update to version 115 or later, Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Mozilla Firefox version before 115 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Block all cookies bypass for localstorage.
- Use-after-free in WebRTC certificate generation.
- Potential use-after-free from compartment mismatch in SpiderMonkey.
- Drag and Drop API may provide access to local system files.
- Fullscreen notification obscured via option element.
- URL spoofing in address bar using RTL characters.
- Insufficient validation of symlinks in the FileSystem API.
- Fullscreen notification obscured.
- Lack of warning when opening Diagcab files.
- Use-after-free in 'NotifyOnHistoryReload'.
- Full-screen mode exit prevention.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates (mfsa_2023-22_2023-24) - Windows`
OID:1.3.6.1.4.1.25623.1.0.832094
Version used: `2023-07-10T08:07:43Z`

References
`cve: CVE-2023-3482`
`cve: CVE-2023-37201`
`cve: CVE-2023-37202`
`cve: CVE-2023-37203`
`cve: CVE-2023-37204`
`cve: CVE-2023-37205`
`cve: CVE-2023-37206`
`cve: CVE-2023-37207`
`cve: CVE-2023-37208`
`cve: CVE-2023-37209`
`cve: CVE-2023-37210`
`cve: CVE-2023-37211`
`cve: CVE-2023-37212`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-22/`
`cert-bund: WID-SEC-2023-1663`
`dfn-cert: DFN-CERT-2023-1611`
`dfn-cert: DFN-CERT-2023-1564`
`dfn-cert: DFN-CERT-2023-1531`
`dfn-cert: DFN-CERT-2023-1530`

High (CVSS: 10.0)
NVT: Adobe Reader/Acrobat 'U3D' Component Memory Corruption Vulnerability (APSA11-04, APSB11-30) - Windows

Summary
Adobe Reader/Acrobat is prone to a memory corruption vulnerability.

Vulnerability Detection Result
```
Installed version: 10.0.0
Fixed version:     9.4.7. For 10.x see the references.
Installation
path / port:       C:\Program Files (x86)\Adobe\Reader 10.0\Reader\
```

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the affected application or cause a denial of service.

Solution:
Solution type: VendorFix
- Update to Adobe Reader or Acrobat version 9.4.7 or later
- For 10.x versions see the references

Affected Software/OS
- Adobe Reader versions 9.x through 9.4.6 and 10.x through 10.1.1
- Adobe Acrobat versions 9.x through 9.4.6 and 10.x through 10.1.1

Vulnerability Insight
The flaw is due to an unspecified error while handling U3D data.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader/Acrobat 'U3D' Component Memory Corruption Vulnerability (APSA11-04. ↪..`
OID:1.3.6.1.4.1.25623.1.0.802542
Version used: `2023-05-17T09:09:49Z`

References
```
cve: CVE-2011-2462
cve: CVE-2011-4369
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://secunia.com/advisories/47133/
url: http://www.securityfocus.com/bid/50922
url: http://www.securityfocus.com/bid/51092
url: https://www.adobe.com/support/security/advisories/apsa11-04.html
url: http://www.adobe.com/support/security/bulletins/apsb11-30.html
dfn-cert: DFN-CERT-2012-0092
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-0064
dfn-cert: DFN-CERT-2012-0062
dfn-cert: DFN-CERT-2012-0061
dfn-cert: DFN-CERT-2011-1873

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates (mfsa2023-13) - Windows

Summary
Mozilla Firefox and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 112
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to execute arbitrary code, disclose sensitive information and conduct spoofing attacks.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 112 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 112 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Mozilla Maintenance Service Write-lock bypass
- Fullscreen notification obscured
- Double-free in libwebp
- Potential Memory Corruption following Garbage Collector compaction
- Invalid free from JavaScript code
- Data Races in font initialization code
- Directory information could have been leaked to WebExtensions
- Content-Disposition filename truncation leads to Reflected File Download
- Iframe sandbox bypass using redirects and sourceMappingUrls
- Bypass of file download extension restrictions
- Use-after-free in debugging APIs
- Memory Corruption in garbage collector
- Windows Save As dialog resolved environment variables
- Secure document cookie could be spoofed with insecure cookie

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates (mfsa2023-13) - Windows
OID:1.3.6.1.4.1.25623.1.0.832110
Version used: 2023-04-18T10:19:20Z

References

cve: CVE-2023-29532
cve: CVE-2023-29533
cve: CVE-2023-29535
cve: CVE-2023-29536
cve: CVE-2023-29537
cve: CVE-2023-29538
cve: CVE-2023-29539
cve: CVE-2023-29540
cve: CVE-2023-29542
cve: CVE-2023-29543
cve: CVE-2023-29544
cve: CVE-2023-29545
cve: CVE-2023-29547
cve: CVE-2023-29548
cve: CVE-2023-29549
cve: CVE-2023-29550
cve: CVE-2023-29551
cve: CVE-2023-1999
url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1133
cert-bund: WID-SEC-2023-0941
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0998
dfn-cert: DFN-CERT-2023-0937
dfn-cert: DFN-CERT-2023-0805
dfn-cert: DFN-CERT-2023-0804

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update (MFSA2022-40) - Windows

Summary

Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 97.0
Fixed version: 105
Installation
path / port: C:\Program Files\Mozilla Firefox

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, and leak memory on affected system.

Solution:
Solution type: VendorFix
Update to version 105 or later.

Affected Software/OS
Mozilla Firefox version before 105 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- Out of bounds read when decoding H264.
- Bypassing FeaturePolicy restrictions on transient pages.
- Data-race when parsing non-UTF-8 URLs in threads.
- Bypassing Secure Context restriction for cookies with __Host and __Secure prefix.
- Content-Security-Policy base-uri bypass.
- Incoherent instruction cache when building WASM on ARM64.
- Memory safety bugs.
- Use-after-free in WebGL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update (MFSA2022-40) - Windows`
OID:1.3.6.1.4.1.25623.1.0.826475
Version used: `2022-12-14T10:20:42Z`

References
`cve: CVE-2022-40959`
`cve: CVE-2022-40960`
`cve: CVE-2022-40958`
`cve: CVE-2022-40962`
`cve: CVE-2022-40956`
`cve: CVE-2022-40957`
`cve: CVE-2022-3266`
`cve: CVE-2022-46880`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-40`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2319`
`cert-bund: WID-SEC-2022-1497`
`cert-bund: WID-SEC-2022-1484`
`dfn-cert: DFN-CERT-2023-0150`
`dfn-cert: DFN-CERT-2022-2836`
`dfn-cert: DFN-CERT-2022-2828`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2551
dfn-cert: DFN-CERT-2022-2104
dfn-cert: DFN-CERT-2022-2090

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa_2023-18_2023-20)-Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 114
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to execute arbitrary code, bypass security restrictions and cause denial of service on an affected system

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 114 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 114 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Click-jacking certificate exceptions through rendering lag.
- Site-isolation bypass on sites that allow open redirects to data: urls.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Update(mfsa_2023-18_2023-20)-Windows
OID:1.3.6.1.4.1.25623.1.0.832203
Version used: 2023-06-14T05:05:19Z

References
cve: CVE-2023-34414
cve: CVE-2023-34415
cve: CVE-2023-34416
cve: CVE-2023-34417

... continues on next page ...

... continued from previous page ...

url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-20/
cert-bund: WID-SEC-2023-1414
cert-bund: WID-SEC-2023-1385
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1564
dfn-cert: DFN-CERT-2023-1340
dfn-cert: DFN-CERT-2023-1335
dfn-cert: DFN-CERT-2023-1305

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update (MFSA2022-47) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 107
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, cause denial of service, disclose sensitive information and conduct spoofing on affected system.

Solution:
Solution type: VendorFix
Update to version 107 or later.

Affected Software/OS
Mozilla Firefox version prior to 107 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Service Workers might have learned size of cross-origin media files.
- Fullscreen notification bypass.
- Use-after-free in InputStream implementation.
- Use-after-free of a JavaScript Realm.
- Loading fonts on workers was not thread-safe.
- Fullscreen notification bypass via windowName.
- Use-after-free in Garbage Collection.
- ServiceWorker-intercepted requests bypassed SameSite cookie policy.
- Cross-Site Tracing was possible via non-standard override headers.
- Use-after-free vulnerability in expat.
- Downloaded file may have been saved with malicious extension.
- Keystroke Side-Channel Leakage.

... continues on next page ...

... continued from previous page ...

- Service Workers in Private Browsing Mode may have been written to disk.
- Custom mouse cursor could have been drawn over browser UI.
- Deleting a security exception did not take effect immediately.
- Iframe contents could be rendered outside the iframe.
- Memory safety bugs.
- Use-after-free in WebGL.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Mozilla Firefox Security Update (MFSA2022-47) - Windows`

OID:1.3.6.1.4.1.25623.1.0.826701

Version used: `2022-12-14T10:20:42Z`

References

`cve: CVE-2022-45403`
`cve: CVE-2022-45404`
`cve: CVE-2022-45405`
`cve: CVE-2022-45406`
`cve: CVE-2022-45407`
`cve: CVE-2022-45408`
`cve: CVE-2022-45409`
`cve: CVE-2022-45410`
`cve: CVE-2022-45411`
`cve: CVE-2022-40674`
`cve: CVE-2022-45415`
`cve: CVE-2022-45416`
`cve: CVE-2022-45417`
`cve: CVE-2022-45418`
`cve: CVE-2022-45419`
`cve: CVE-2022-45420`
`cve: CVE-2022-45421`
`cve: CVE-2022-46882`
`cve: CVE-2022-46883`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/`
`cert-bund: WID-SEC-2023-1728`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-2319`
`cert-bund: WID-SEC-2022-2055`
`cert-bund: WID-SEC-2022-1504`
`dfn-cert: DFN-CERT-2023-1162`
`dfn-cert: DFN-CERT-2023-0666`
`dfn-cert: DFN-CERT-2023-0150`
`dfn-cert: DFN-CERT-2023-0120`
`dfn-cert: DFN-CERT-2022-2836`
`dfn-cert: DFN-CERT-2022-2828`
`dfn-cert: DFN-CERT-2022-2821`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2664
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2576
dfn-cert: DFN-CERT-2022-2575
dfn-cert: DFN-CERT-2022-2344
dfn-cert: DFN-CERT-2022-2343
dfn-cert: DFN-CERT-2022-2264
dfn-cert: DFN-CERT-2022-2218
dfn-cert: DFN-CERT-2022-2207
dfn-cert: DFN-CERT-2022-2120

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa2022-28) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 103
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 103 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 103 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Mouse Position spoofing with CSS transforms.
- Directory indexes for bundled resources reflected URL parameters.
- Opening local <code>.lnk</code> files could cause unexpected network loads.
- Preload Cache Bypasses Subresource Integrity.
- Performance API leaked whether a cross-site resource is redirecting.
- Memory safety bugs

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: Mozilla Firefox Security Update(mfsa2022-28) - Windows
OID:1.3.6.1.4.1.25623.1.0.821196
Version used: 2022-08-26T10:12:16Z

References
cve: CVE-2022-36319
cve: CVE-2022-2505
cve: CVE-2022-36318
cve: CVE-2022-36314
cve: CVE-2022-36315
cve: CVE-2022-36316
cve: CVE-2022-36320
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-28
cert-bund: WID-SEC-2022-0859
cert-bund: WID-SEC-2022-0837
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2225
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1679
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1654

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa2022-33) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 104
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and memory leak on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 104 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 104 on Windows.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws exist due to,
- Address bar spoofing via XSLT error handling.
- Cross-origin XSLT Documents would have inherited the parent's permissions.
- Attacker could write a value to a zero-length array.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update(mfsa2022-33) - Windows`
OID:1.3.6.1.4.1.25623.1.0.826419
Version used: `2022-08-26T10:12:16Z`

References
`cve: CVE-2022-38472`
`cve: CVE-2022-38473`
`cve: CVE-2022-38478`
`cve: CVE-2022-38475`
`cve: CVE-2022-38477`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-33`
`cert-bund: WID-SEC-2022-1167`
`dfn-cert: DFN-CERT-2022-2323`
`dfn-cert: DFN-CERT-2022-2225`
`dfn-cert: DFN-CERT-2022-2179`
`dfn-cert: DFN-CERT-2022-2056`
`dfn-cert: DFN-CERT-2022-1865`
`dfn-cert: DFN-CERT-2022-1864`

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa_2022-09) - Windows

Summary
Mozilla Firefox is prone to multiple use-after-free vulnerabilities.

Vulnerability Detection Result
```
Installed version: 97.0
Fixed version:     97.0.2
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact
Successful exploitation can lead to arbitrary code execution or allow an attacker to gain remote code execution capabilities and cause denial of service condition.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Mozilla Firefox version 97.0.2 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 97.0.2 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Use-after-free in WebGPU IPC Framework.
- Use-after-free in XSLT parameter processing.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update(mfsa_2022-09) - Windows`
OID:1.3.6.1.4.1.25623.1.0.820017
Version used: `2022-08-09T10:11:17Z`

References
```
cve: CVE-2022-26485
cve: CVE-2022-26486
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1032
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0269
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0505
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Update(mfsa_2022-51_2022-53)-Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 97.0
Fixed version:     108
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 108 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 108 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- libusrsctp library out of date.
- Firefox did not implement the CSP directive unsafe-hashes.
- Drag and Dropped Filenames could have been truncated to malicious extensions.
- Fullscreen notification bypass.
- Memory safety bugs fixed in Firefox 108 and Firefox ESR 102.6.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update(mfsa_2022-51_2022-53)-Windows`
OID:1.3.6.1.4.1.25623.1.0.826816
Version used: `2022-12-19T10:12:02Z`

References
`cve: CVE-2022-46871`
`cve: CVE-2022-46873`
`cve: CVE-2022-46874`
`cve: CVE-2022-46877`
`cve: CVE-2022-46878`
`cve: CVE-2022-46879`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2319`
`dfn-cert: DFN-CERT-2023-0408`
`dfn-cert: DFN-CERT-2023-0150`
`dfn-cert: DFN-CERT-2023-0146`
`dfn-cert: DFN-CERT-2023-0104`
`dfn-cert: DFN-CERT-2022-2932`
`dfn-cert: DFN-CERT-2022-2836`
`dfn-cert: DFN-CERT-2022-2828`

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa_2023-16_2023-17)-Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 97.0`
`Fixed version: 113`
`Installation path / port: C:\Program Files\Mozilla Firefox`

Impact
Successful exploitation allow attackers to disclose sensitive information, execute arbitrary code and cause denial of service condition.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 113 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 113 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Browser prompts could have been obscured by popups.
- Crash in RLBox Expat driver.
- Potential permissions request bypass via clickjacking.
- Leak of script base URL in service workers via import().
- Persistent DoS via favicon image.
- Incorrect principal object ordering.
- Content process crash due to invalid wasm code.
- Potential spoof due to obscured address bar.
- Potential memory corruption in FileReader::DoReadData().
- Potential DoS via exposed protocol handlers.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa_2023-16_2023-17)-Windows`
OID:1.3.6.1.4.1.25623.1.0.832076
Version used: `2023-05-12T10:50:26Z`

References
`cve: CVE-2023-32205`
`cve: CVE-2023-32206`
`cve: CVE-2023-32207`
`cve: CVE-2023-32208`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2023-32209
cve: CVE-2023-32210
cve: CVE-2023-32211
cve: CVE-2023-32212
cve: CVE-2023-32213
cve: CVE-2023-32214
cve: CVE-2023-32215
cve: CVE-2023-32216
url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-16/
cert-bund: WID-SEC-2023-1201
cert-bund: WID-SEC-2023-1172
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-1090
dfn-cert: DFN-CERT-2023-1040
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa_2023-07_2023-11)-Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 97.0
Fixed version:     111
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact
Successful exploitation allow attackers to disclose sensitive information, execute arbitrary code and cause denial of service condition.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 111 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 111 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- User Interface lockup with messages combining S/MIME and OpenPGP.
- Content security policy leak in violation reports using iframes.
- Screen hijack via browser fullscreen mode.
- Arbitrary memory write via PKCS 12 in NSS.
- Potential use-after-free from compartment mismatch in SpiderMonkey.
- Invalid downcast in SVGUtils::SetupStrokeGeometry.

... continues on next page ...

... continued from previous page ...

- Printing on Windows could potentially crash Thunderbird with some device drivers.
- Extensions could have opened external schemes without user knowledge.
- Out of bounds memory write from EncodeInputStream.
- Opening local .url files could cause unexpected network loads.
- Web Crypto ImportKey crashes tab.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Updates(mfsa_2023-07_2023-11)-Windows`
OID:1.3.6.1.4.1.25623.1.0.832074
Version used: `2023-05-12T10:50:26Z`

References
`cve: CVE-2023-25750`
`cve: CVE-2023-25751`
`cve: CVE-2023-28160`
`cve: CVE-2023-28164`
`cve: CVE-2023-28161`
`cve: CVE-2023-28162`
`cve: CVE-2023-25752`
`cve: CVE-2023-28163`
`cve: CVE-2023-28176`
`cve: CVE-2023-28177`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0941`
`cert-bund: WID-SEC-2023-0673`
`cert-bund: WID-SEC-2023-0643`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0805`
`dfn-cert: DFN-CERT-2023-0741`
`dfn-cert: DFN-CERT-2023-0738`
`dfn-cert: DFN-CERT-2023-0579`
`dfn-cert: DFN-CERT-2023-0557`

High (CVSS: 10.0)
NVT: Mozilla Firefox Security Updates(mfsa_2023-04_2023-06)-Windows

Summary
Mozilla Firefox and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 97.0`
`Fixed version: 110`
`Installation`

... continues on next page ...

... continued from previous page ...

path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to execute arbitrary code, disclose sensitive information and conduct spoofing attacks.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 110 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 110 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Content security policy leak in violation reports using iframes.
- Screen hijack via browser fullscreen mode.
- Arbitrary memory write via PKCS 12 in NSS.
- Potential use-after-free from compartment mismatch in SpiderMonkey.
- Invalid downcast in SVGUtils::SetupStrokeGeometry.
- Use-after-free in mozilla::dom::ScriptLoadContext:: ScriptLoadContext.
- Extensions could have opened external schemes without user knowledge.
- Out of bounds memory write from EncodeInputStream.
- Web Crypto ImportKey crashes tab.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates(mfsa_2023-04_2023-06)-Windows
OID:1.3.6.1.4.1.25623.1.0.832012
Version used: 2023-03-06T10:19:58Z

References
cve: CVE-2023-25728
cve: CVE-2023-25730
cve: CVE-2023-0767
cve: CVE-2023-25745
cve: CVE-2023-25735
cve: CVE-2023-25737
cve: CVE-2023-25739
cve: CVE-2023-25744
cve: CVE-2023-25729
cve: CVE-2023-25732
cve: CVE-2023-25742
cve: CVE-2023-25741
cve: CVE-2023-25731
cve: CVE-2023-25733

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-25736
url: https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0407
cert-bund: WID-SEC-2023-0385
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0843
dfn-cert: DFN-CERT-2023-0411
dfn-cert: DFN-CERT-2023-0408
dfn-cert: DFN-CERT-2023-0395
dfn-cert: DFN-CERT-2023-0394
dfn-cert: DFN-CERT-2023-0340

High (CVSS: 9.8)
NVT: VLC Media Player QuickTime IMA File Denial of Service Vulnerability June16 (Windows)

Summary
VLC media player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.2.4

Impact
Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted QuickTime IMA file.

Solution:
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 2.2.4 or later.

Affected Software/OS
VideoLAN VLC media player before 2.2.4 on Windows.

Vulnerability Insight
The flaw is due to a buffer overflow vulnerability in the 'DecodeAdpcmImaQT' function in 'modules/codec/adpcm.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player QuickTime IMA File Denial of Service Vulnerability June16 (Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.808221

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-21T05:05:22Z

References
cve: CVE-2016-5108
url: http://www.securitytracker.com/id/1036009
url: http://www.videolan.org/security/sa1601.html
cert-bund: CB-K16/0963
cert-bund: CB-K16/0962
cert-bund: CB-K16/0853
dfn-cert: DFN-CERT-2016-1016
dfn-cert: DFN-CERT-2016-1015
dfn-cert: DFN-CERT-2016-0908

High (CVSS: 9.8)
NVT: VLC Media Player 'avcodec picture copy' Heap Buffer Overflow Vulnerability (Windows)

Summary
VLC media player is prone to a heap-based buffer over-read vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 3.0.8
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow attackers to cause a denial-of-service condition, denying service to legitimate users and may also be able to execute arbitrary code.

Solution:
Solution type: VendorFix
Update to version 3.0.8 or later.

Affected Software/OS
VideoLAN VLC media player version through 3.0.7 on Windows.

Vulnerability Insight
The flaw exists due to a heap-based buffer over-read error in lavc_CopyPicture in modules/codec/avcodec/video.c due to insufficient validation of width and height.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player 'avcodec picture copy' Heap Buffer Overflow Vulnerability (Win.
↪..
OID:1.3.6.1.4.1.25623.1.0.815429

... continues on next page ...

. . . continued from previous page . . .

Version used: 2022-04-20T03:02:11Z

References
cve: CVE-2019-13962
url: https://www.videolan.org/security/sb-vlc308.html
url: https://trac.videolan.org/vlc/ticket/22240
cert-bund: CB-K19/0737
cert-bund: CB-K19/0654
dfn-cert: DFN-CERT-2019-1753
dfn-cert: DFN-CERT-2019-1666

High (CVSS: 9.8)
NVT: Adobe Reader/Acrobat Multiple Memory Corruption Vulnerabilities (apsb12-01) - Windows

Summary
Adobe products are prone to multiple memory corruption vulnerabilities.

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 9.5 or 10.1.2
Installation
path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the affected application or cause a denial of service.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 9.5 or 10.1.2 or later.
Upgrade to Adobe Acrobat version 9.5 or 10.1.2 or later.

Affected Software/OS
Adobe Reader versions 9.x through 9.4.7 and 10.x through 10.1.1 on Windows.
Adobe Acrobat versions 9.x through 9.4.7 and 10.x through 10.1.1 on Windows.

Vulnerability Insight
The flaws are due to
- An unspecified error can be exploited to corrupt memory.
- A signedness error in rt3d.dll when parsing certain BMP image content can be exploited to cause a heap-based buffer overflow via a specially crafted BMP image embedded in a PDF document.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

... continued from previous page ...

Details: Adobe Reader/Acrobat Multiple Memory Corruption Vulnerabilities (apsb12-01) - W.
↪..
OID:1.3.6.1.4.1.25623.1.0.802558
Version used: 2022-10-06T10:41:20Z

References
cve: CVE-2011-4370
cve: CVE-2011-4371
cve: CVE-2011-4372
cve: CVE-2011-4373
url: http://secunia.com/advisories/45852/
url: http://www.securityfocus.com/bid/51348
url: http://www.securityfocus.com/bid/51349
url: http://www.securityfocus.com/bid/51350
url: http://www.securityfocus.com/bid/51351
url: http://securitytracker.com/id/1026496
url: http://www.adobe.com/support/security/bulletins/apsb12-01.html
dfn-cert: DFN-CERT-2012-0064

High (CVSS: 9.8)
NVT: VLC Media Player 'audio.c' Heap-Based Buffer Overflow Vulnerability (Windows)

Summary
VLC media player is prone to a heap overflow vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.1.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code.

Solution:
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 2.1.5 or later.

Affected Software/OS
VideoLAN VLC media player before 2.1.5 on Windows.

Vulnerability Insight
The flaw is due to error in the transcode module that may allow a corrupted stream to overflow buffers on the heap. With a non-malicious input, this could lead to heap corruption and a crash.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: VLC Media Player 'audio.c' Heap-Based Buffer Overflow Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.810721
Version used: 2022-04-13T11:57:07Z

References
cve: CVE-2014-6440
url: http://seclists.org/oss-sec/2015/q1/751
url: http://www.securityfocus.com/bid/72950
url: http://billblough.net/blog/2015/03/04/cve-2014-6440-heap-overflow-in-vlc-tr
↪anscode-module
url: http://www.videolan.org/developers/vlc-branch/NEWS

High (CVSS: 9.8)
NVT: VLC Media Player Multiple Vulnerabilities Jun19 (Windows)

Summary
VLC media player is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 3.0.7
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the affected application, cause denial of service or launch other attacks.

Solution:
Solution type: VendorFix
Upgrade to version 3.0.7 or later. Please see the references for more information.

Affected Software/OS
VideoLAN VLC media player version before 3.0.7 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- An out of bounds write error in faad2 library.
- Multiple out-of-band read errors.
- Multiple heap overflow errors.
- A NULL pointer dereference error.
- Multiple use-after-free issues.
- An integer underflow error.
- Multiple integer overflow errors.
- A division by zero error.

... continues on next page ...

... continued from previous page ...

- A floating point exception error.
- An infinite loop error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Multiple Vulnerabilities Jun19 (Windows)
OID:1.3.6.1.4.1.25623.1.0.815204
Version used: 2021-10-07T07:48:17Z

References
cve: CVE-2019-5439
cve: CVE-2019-12874
url: https://www.videolan.org/developers/vlc-branch/NEWS
url: https://www.videolan.org/security/sa1901.html
url: https://www.pentestpartners.com/security-blog/double-free-rce-in-vlc-a-hong
↪gfuzz-how-to/
url: https://hackerone.com/reports/484398
cert-bund: CB-K19/0507
dfn-cert: DFN-CERT-2019-1666
dfn-cert: DFN-CERT-2019-1534

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat Multiple BOF Vulnerabilities June-2011 (Windows)

Summary
Adobe Reader/Acrobat is prone to multiple buffer overflow vulnerabilities.

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 10.1, 9.4.5 or 8.3
Installation
path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\

Impact
Successful exploitation will let local attackers to application to crash and potentially take control of the affected system.

Solution:
Solution type: VendorFix
Upgrade to Adobe Acrobat and Reader version 10.1, 9.4.5 or 8.3 or later.

Affected Software/OS
Adobe Acrobat version 8.0 to 8.2.6, 9.0 to 9.4.4 and 10.0 to 10.0.3
Adobe Reader version 8.0 to 8.2.6, 9.0 to 9.4.4 and 10.0 to 10.0.3

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws are caused by buffer overflow errors in the applications, which allows attackers to execute arbitrary code via unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader and Acrobat Multiple BOF Vulnerabilities June-2011 (Windows)
OID:1.3.6.1.4.1.25623.1.0.802110
Version used: 2022-04-28T13:38:57Z

References
cve: CVE-2011-2094
cve: CVE-2011-2095
cve: CVE-2011-2096
cve: CVE-2011-2097
cve: CVE-2011-2098
cve: CVE-2011-2099
cve: CVE-2011-2100
cve: CVE-2011-2101
cve: CVE-2011-2104
cve: CVE-2011-2105
cve: CVE-2011-2106
url: http://www.adobe.com/support/security/bulletins/apsb11-16.html
url: http://www.securityfocus.com/bid/48240
url: http://www.securityfocus.com/bid/48242
url: http://www.securityfocus.com/bid/48243
url: http://www.securityfocus.com/bid/48244
url: http://www.securityfocus.com/bid/48245
url: http://www.securityfocus.com/bid/48246
url: http://www.securityfocus.com/bid/48248
url: http://www.securityfocus.com/bid/48249
url: http://www.securityfocus.com/bid/48251
url: http://www.securityfocus.com/bid/48252
url: http://www.securityfocus.com/bid/48255
url: http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Wind
↪ows
dfn-cert: DFN-CERT-2011-0950

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Unspecified Vulnerabilities (Aug 2012) - Windows

Summary
Adobe Reader is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Installed version: 10.0.0

... continues on next page ...

... continued from previous page ...

Fixed version: 9.5.3/10.1.5

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the affected application.

Solution:
Solution type: VendorFix
Update to version 9.5.3, 10.1.5 or later.

Affected Software/OS
Adobe Reader versions 9.x through 9.5.2 and 10.x through 10.1.4 on Windows.

Vulnerability Insight
The flaws are due to an unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader Multiple Unspecified Vulnerabilities (Aug 2012) - Windows
OID:1.3.6.1.4.1.25623.1.0.802954
Version used: 2023-05-04T09:51:03Z

References
cve: CVE-2012-4363
url: http://secunia.com/advisories/50290
url: http://www.securityfocus.com/bid/55055

High (CVSS: 9.3)
NVT: VLC Media Player TiVo Demuxer Double Free Vulnerability (Windows)

Summary
VLC Media Player is prone to double free vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 1.1.13
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow an attacker to crash an affected application and denying service to legitimate users.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade VLC media player to 1.1.13 or later.

Affected Software/OS
VLC media player version 0.9.0 to 1.1.12 on Windows

Vulnerability Insight
The flaw is due to a double-free error within the 'get_chunk_header()' function in 'modules/demux/ty.c' of the TiVo demuxer when opening a specially crafted TiVo (*.ty) file.

Vulnerability Detection Method
Details: `VLC Media Player TiVo Demuxer Double Free Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.802480
Version used: `2022-04-27T12:01:52Z`

References
`cve: CVE-2012-0023`
`cve: CVE-2011-5231`
`url: http://secunia.com/advisories/47325`
`url: http://www.securityfocus.com/bid/51147`
`url: http://www.securityfocus.com/bid/51231`
`url: http://securitytracker.com/id?1026449`
`url: http://xforce.iss.net/xforce/xfdb/71916`
`url: http://www.videolan.org/security/sa1108.html`

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Unspecified Vulnerabilities -01 Feb13 (Windows)

Summary
Adobe Reader is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow attacker to execute arbitrary code or cause a denial of service via a crafted PDF document.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 9.5.4, 10.1.6, 11.0.02 or later.

Affected Software/OS
Adobe Reader Version 9.x prior to 9.5.4 on Windows
Adobe Reader X Version 10.x prior to 10.1.6 on Windows

... continues on next page ...

... continued from previous page ...

Adobe Reader XI Version 11.x prior to 11.0.02 on Windows

Vulnerability Insight
The flaws are due to unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Multiple Unspecified Vulnerabilities -01 Feb13 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.803415
Version used: `2022-08-09T10:11:17Z`

References
`cve: CVE-2013-0640`
`cve: CVE-2013-0641`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: http://secunia.com/advisories/52196`
`url: http://www.securityfocus.com/bid/57931`
`url: http://www.securityfocus.com/bid/57947`
`url: http://www.adobe.com/support/security/advisories/apsa13-02.html`
`url: http://blogs.adobe.com/psirt/2013/02/adobe-reader-and-acrobat-vulnerability`
`↪-report.html`
`dfn-cert: DFN-CERT-2013-0434`
`dfn-cert: DFN-CERT-2013-0411`
`dfn-cert: DFN-CERT-2013-0402`
`dfn-cert: DFN-CERT-2013-0392`
`dfn-cert: DFN-CERT-2013-0381`
`dfn-cert: DFN-CERT-2013-0309`

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat Multiple Vulnerabilities February-2011 (Windows)

Summary
Adobe Reader/Acrobat is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 10.0.0`
`Fixed version: 10.0.1, 9.4.2 or 8.2.6`
`Installation`
`path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\`

Impact
Successful exploitation will let local attackers to obtain elevated privileges, or by remote attackers to inject scripting code, or execute arbitrary commands by tricking a user into opening a malicious PDF document.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Adobe Acrobat and Reader version 10.0.1, 9.4.2 or 8.2.6.

Affected Software/OS
Adobe Acrobat X version 10.0
Adobe Acrobat version 9.4.1 and prior
Adobe Acrobat version 8.2.5 and prior
Adobe Reader X version 10.0
Adobe Reader version 9.4.1 and prior
Adobe Reader version 8.2.5 and prior

Vulnerability Insight
Multiple flaws are caused by insecure permissions, input validation errors, memory corruptions, and buffer overflow errors when processing malformed contents within a PDF document.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader and Acrobat Multiple Vulnerabilities February-2011 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.801844
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-0602`
`cve: CVE-2010-4091`
`cve: CVE-2011-0562`
`cve: CVE-2011-0563`
`cve: CVE-2011-0564`
`cve: CVE-2011-0565`
`cve: CVE-2011-0566`
`cve: CVE-2011-0567`
`cve: CVE-2011-0568`
`cve: CVE-2011-0570`
`cve: CVE-2011-0585`
`cve: CVE-2011-0586`
`cve: CVE-2011-0587`
`cve: CVE-2011-0588`
`cve: CVE-2011-0589`
`cve: CVE-2011-0590`
`cve: CVE-2011-0591`
`cve: CVE-2011-0592`
`cve: CVE-2011-0593`
`cve: CVE-2011-0594`
`cve: CVE-2011-0595`
`cve: CVE-2011-0596`
`cve: CVE-2011-0598`
`cve: CVE-2011-0599`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2011-0600
cve: CVE-2011-0603
cve: CVE-2011-0604
cve: CVE-2011-0605
cve: CVE-2011-0606
url: http://www.vupen.com/english/advisories/2011/0337
url: http://www.securityfocus.com/bid/46146
url: http://www.adobe.com/support/security/bulletins/apsb11-03.html
dfn-cert: DFN-CERT-2011-0776
dfn-cert: DFN-CERT-2011-0753
dfn-cert: DFN-CERT-2011-0318
dfn-cert: DFN-CERT-2011-0252
dfn-cert: DFN-CERT-2011-0170
dfn-cert: DFN-CERT-2010-1661
dfn-cert: DFN-CERT-2010-1637
dfn-cert: DFN-CERT-2010-1581
```

High (CVSS: 9.3)
NVT: Adobe Reader/Acrobat Security Bypass Vulnerability (apsb11-16) - Windows

Summary
Adobe Reader/Acrobat is prone to a security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 10.0.0
Fixed version:     10.1
Installation
path / port:       C:\Program Files (x86)\Adobe\Reader 10.0\Reader\
```

Impact
Successful exploitation allows attackers to bypass intended security restrictions, which may leads to the other attacks.

Solution:
Solution type: VendorFix
Upgrade to Adobe Acrobat and Reader version 10.1 or later.

Affected Software/OS
Adobe Reader version 10.0.1 and prior.
Adobe Acrobat version 10.0.1 and prior.

Vulnerability Insight
The flaw is caused by an unknown vectors, allows attackers to bypass intended access restriction.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: Adobe Reader/Acrobat Security Bypass Vulnerability (apsb11-16) - Windows
OID:1.3.6.1.4.1.25623.1.0.902387
Version used: 2022-04-28T13:38:57Z

References
cve: CVE-2011-2102
url: http://www.adobe.com/support/security/bulletins/apsb11-16.html
url: http://www.securityfocus.com/bid/48253
dfn-cert: DFN-CERT-2011-0950

High (CVSS: 9.3)
NVT: VLC Media Player XSPF Playlist Integer Overflow Vulnerability - Windows

Summary
VLC Media Player is prone to an integer overflow vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 1.1.10
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation could allow attackers to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

Solution:
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.10 or later.

Affected Software/OS
VLC media player version 0.8.5 through 1.1.9

Vulnerability Insight
The flaw is due to an integer overflow in XSPF playlist file parser, which allows attackers to execute arbitrary code via unspecified vectors.

Vulnerability Detection Method
Details: VLC Media Player XSPF Playlist Integer Overflow Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.902603
Version used: 2022-04-28T13:38:57Z

References
cve: CVE-2011-2194
url: http://www.videolan.org/security/sa1104.html

... continues on next page ...

. . . continued from previous page . . .

url: http://www.securityfocus.com/bid/48171
dfn-cert: DFN-CERT-2011-0907

High (CVSS: 9.3)
NVT: Adobe Reader Out-of-bounds Vulnerability Feb15 (Windows)

Summary
Adobe Reader is prone to unspecified Out-of-bounds error vulnerability.

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 10.1.13

Impact
Successful exploitation will allow context-dependent attacker to cause a crash or potentially disclose memory contents.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.13 or 11.0.10 or later.

Affected Software/OS
Adobe Reader 10.x before 10.1.13 and Adobe Reader 11.x before 11.0.10 on Windows.

Vulnerability Insight
The error exists due to an out-of-bounds read flaw in CoolType.dll

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader Out-of-bounds Vulnerability Feb15 (Windows)
OID:1.3.6.1.4.1.25623.1.0.805438
Version used: 2021-10-21T13:57:32Z

References
cve: CVE-2014-9161
url: http://code.google.com/p/google-security-research/issues/detail?id=149
cert-bund: CB-K15/0652
dfn-cert: DFN-CERT-2015-0680

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat Multiple Vulnerabilities (APSB11-24) - Windows

Summary
Adobe Reader/Acrobat is prone to multiple vulnerabilities.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 10.1.1, 9.4.6 or 8.3.1
Installation
path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\

Impact
Successful exploitation will let attackers to execute arbitrary code via unspecified vectors.

Solution:
Solution type: VendorFix
Update to Adobe Acrobat and Reader version 8.3.1, 9.4.6, 10.1.1 or later.

Affected Software/OS
- Adobe Reader versions 8.x through 8.3.0, 9.x through 9.4.5 and 10.x through 10.1
- Adobe Acrobat versions 8.x through 8.3.0, 9.x through 9.4.5 and 10.x through 10.1

Vulnerability Insight
Multiple flaws are due to memory corruptions, and buffer overflow errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Reader and Acrobat Multiple Vulnerabilities (APSB11-24) - Windows
OID:1.3.6.1.4.1.25623.1.0.802166
Version used: 2023-05-17T09:09:49Z

References
cve: CVE-2011-2431
cve: CVE-2011-2432
cve: CVE-2011-2433
cve: CVE-2011-2434
cve: CVE-2011-2435
cve: CVE-2011-2436
cve: CVE-2011-2437
cve: CVE-2011-2438
cve: CVE-2011-2439
cve: CVE-2011-2440
cve: CVE-2011-2441
cve: CVE-2011-2442
url: http://www.adobe.com/support/security/bulletins/apsb11-24.html
url: http://www.securityfocus.com/bid/49572
url: http://www.securityfocus.com/bid/49575
url: http://www.securityfocus.com/bid/49576
url: http://www.securityfocus.com/bid/49577
url: http://www.securityfocus.com/bid/49578

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/49579
url: http://www.securityfocus.com/bid/49580
url: http://www.securityfocus.com/bid/49581
url: http://www.securityfocus.com/bid/49582
url: http://www.securityfocus.com/bid/49583
url: http://www.securityfocus.com/bid/49584
url: http://www.securityfocus.com/bid/49585
dfn-cert: DFN-CERT-2011-1784
dfn-cert: DFN-CERT-2011-1752
dfn-cert: DFN-CERT-2011-1750
dfn-cert: DFN-CERT-2011-1712
dfn-cert: DFN-CERT-2011-1419
```

High (CVSS: 9.3)
NVT: Adobe Products Arbitrary Code Execution Vulnerability (Windows)

Summary
Adobe Acrobat/Reader/Flash Player are prone to a code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 10.0.0
Fixed version:     9.4.4 or 10.0.3
Installation
path / port:       C:\Program Files (x86)\Adobe\Reader 10.0\Reader\
```

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.

Solution:
Solution type: VendorFix
Upgrade adobe flash player to version 10.2.159.1 or later, Update Adobe Reader/Acrobat to version 9.4.4 or 10.0.3 or later.

Affected Software/OS
Adobe Flash Player version 10.2.153.1 and prior on Windows.
Adobe Reader/Acrobat version 9.x to 9.4.3 and 10.x to 10.0.2 on Windows.

Vulnerability Insight
The flaw is due to an error in handling 'SWF' file in adobe flash player and 'Authplay.dll' in Adobe acrobat/reader. which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Products Arbitrary Code Execution Vulnerability (Windows)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.801921
Version used: 2022-08-09T10:11:17Z

References
cve: CVE-2011-0611
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.kb.cert.org/vuls/id/230057
url: http://www.securityfocus.com/bid/47314
url: http://www.adobe.com/support/security/advisories/apsa11-02.html
url: http://blogs.adobe.com/psirt/2011/04/security-advisory-for-adobe-flash-play
↪er-adobe-reader-and-acrobat-apsa11-02.html
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2011-0662
dfn-cert: DFN-CERT-2011-0604
dfn-cert: DFN-CERT-2011-0602
dfn-cert: DFN-CERT-2011-0548

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat 'CoolType.dll' Memory Corruption Vulnerability

Summary
Adobe Reader/Acrobat is prone to memory corruption and remote code execution vulnerabilities.

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 9.4.4. For 10.x see the references.
Installation
path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\

Impact
Successful exploitation will let attackers to crash an affected application or compromise a vulnerable system by tricking a user into opening a specially crafted PDF file.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 9.4.4 or Acrobat 9.4.4 or 10.0.3.
NOTE : No fix available for Adobe Reader X (10.x), vendors are planning to address this issue in next quarterly security update for Adobe Reader.

Affected Software/OS
Adobe Reader version prior to 9.4.4 and 10.x to 10.0.1
Adobe Acrobat version prior to 9.4.4 and 10.x to 10.0.2

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

This issue is caused by a memory corruption error in the 'CoolType' library when processing the malformed Flash content within a PDF document.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader and Acrobat 'CoolType.dll' Memory Corruption Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801933
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-0610`
`url: http://www.vupen.com/english/advisories/2011/0923`
`url: http://www.securityfocus.com/bid/47531`
`url: http://www.adobe.com/support/security/bulletins/apsb11-08.html`
`dfn-cert: DFN-CERT-2011-0662`

High (CVSS: 9.3)
NVT: VLC Media Player Multiple Vulnerabilities - Mar 12 (Windows)

Summary
VLC Media Player is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     2.0.1
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation could allow attackers to cause a denial of service or possibly execute arbitrary code via crafted streams.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.1 or later.

Affected Software/OS
VLC media player version prior to 2.0.1 on Windows

Vulnerability Insight
The flaws are due to multiple buffer overflow errors in the application, which allows remote attackers to execute arbitrary code via crafted MMS:// stream and Real RTSP streams.

Vulnerability Detection Method
Details: `VLC Media Player Multiple Vulnerabilities - Mar 12 (Windows)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.802722
Version used: 2022-02-15T13:40:32Z

References
cve: CVE-2012-1775
cve: CVE-2012-1776
url: http://www.videolan.org/security/sa1201.html
url: http://www.videolan.org/security/sa1202.html

High (CVSS: 9.3)
NVT: VLC Media Player Multiple Vulnerabilities - July 13 (Windows)

Summary
VLC Media Player is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.0.5
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow attackers to overflow buffer, cause denial of service or potentially execution of arbitrary code.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.5 or later.

Affected Software/OS
VLC media player version 2.0.4 and prior on Windows

Vulnerability Insight
Multiple flaws due to:
- Error in 'SHAddToRecentDocs()' function.
- Error due to improper validation of user supplied inputs when handling HTML subtitle files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Multiple Vulnerabilities - July 13 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803900
Version used: 2022-04-25T14:50:49Z

References
cve: CVE-2013-1868

... continues on next page ...

... continued from previous page ...

cve: CVE-2012-5855
url: http://xforce.iss.net/xforce/xfdb/79823
url: http://www.securityfocus.com/bid/56405
url: http://www.securityfocus.com/bid/57079
cert-bund: CB-K14/0835
dfn-cert: DFN-CERT-2014-0871

High (CVSS: 9.3)
NVT: VLC Media Player AMV and NSV Data Processing Memory Corruption vulnerability (Windows)

Summary
VLC Media Player is prone to a memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 1.1.8
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation could allow attackers to execute arbitrary code by tricking a user into opening a malicious file or visiting a specially crafted web page.

Solution:
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.8 or later.

Affected Software/OS
VLC media player version prior to 1.1.8 on Windows.

Vulnerability Insight
The flaw is caused by a memory corruption error in the 'libdirectx' plugin when processing malformed NSV or AMV data, which allows the attackers to execute arbitrary code.

Vulnerability Detection Method
Details: VLC Media Player AMV and NSV Data Processing Memory Corruption vulnerability (W.
↪..
OID:1.3.6.1.4.1.25623.1.0.902406
Version used: 2022-04-28T13:38:57Z

References
cve: CVE-2010-3275
cve: CVE-2010-3276
url: http://secunia.com/advisories/43826

... continues on next page ...

... continued from previous page ...

url: http://www.securityfocus.com/bid/47012
url: http://securitytracker.com/id?1025250
url: http://xforce.iss.net/xforce/xfdb/66259
url: http://www.vupen.com/english/advisories/2011/0759
dfn-cert: DFN-CERT-2011-0521

High (CVSS: 9.3)
NVT: Adobe Products Remote Memory Corruption Vulnerability (APSA11-01) - Windows

Summary
Adobe Acrobat, Adobe Reader or Adobe Flash Player is prone to a memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 10.0.0
Fixed version: 10.0.2
Installation
path / port: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.

Solution:
Solution type: VendorFix
Upgrade to Adobe Flash Player to 10.2.153.1 or later and upgrade Adobe Reader/Acrobat to 10.0.2.

Affected Software/OS
Adobe Flash Player version 10.2.152.33 and prior on Windows.
Adobe Reader/Acrobat version 9.x to 9.4.2 and 10.x to 10.0.1 on Windows.

Vulnerability Insight
The flaw is due to an error in handling 'SWF' file in adobe flash player and 'Authplay.dll' in Adobe acrobat/reader. which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Adobe Products Remote Memory Corruption Vulnerability (APSA11-01) - Windows
OID:1.3.6.1.4.1.25623.1.0.902400
Version used: 2022-08-09T10:11:17Z

References
cve: CVE-2011-0609

... continues on next page ...

... continued from previous page ...

```
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.adobe.com/support/security/bulletins/apsb11-06.html
url: http://www.securityfocus.com/bid/46860
url: http://www.adobe.com/support/security/advisories/apsa11-01.html
dfn-cert: DFN-CERT-2011-0492
dfn-cert: DFN-CERT-2011-0423
dfn-cert: DFN-CERT-2011-0418
dfn-cert: DFN-CERT-2011-0413
dfn-cert: DFN-CERT-2011-0371
```

High (CVSS: 8.8)
NVT: VLC Media Player 'MP4 Demux Module' DoS Vulnerability (Windows)

Summary
VLC media player is prone to a denial of service vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     3.0.1
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation will allow remote attackers to cause a denial-of-service condition. Given the nature of this issue, attackers may also be able to execute arbitrary code, but this has not been confirmed.

Solution:
Solution type: VendorFix
Update to version 3.0.1 or later

Affected Software/OS
VideoLAN VLC media player 2.2.8 and prior on Windows.

Vulnerability Insight
The flaw is due to a type conversion error in 'modules/demux/mp4/libmp4.c' in the MP4 demux module leading to an invalid free, because the type of a box may be changed between a read operation and a free operation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player 'MP4 Demux Module' DoS Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812504
Version used: `2023-07-14T16:09:27Z`

... continues on next page ...

. . . continued from previous page . . .

References
cve: CVE-2017-17670
url: http://openwall.com/lists/oss-security/2017/12/15/1
url: http://www.securityfocus.com/bid/102214
dfn-cert: DFN-CERT-2018-0957

High (CVSS: 8.0)
NVT: VLC Media Player MKV Files Arbitrary Code Execution Vulnerability (Windows)

Summary
VLC media player is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 3.0.3
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow attackers to execute arbitrary code in the context of the logged-in user and failed exploit attempts will likely result in denial of service conditions.

Solution:
Solution type: VendorFix
Update to version 3.0.3 or above. Please see the references for more information.

Affected Software/OS
VideoLAN VLC media player versions through 2.2.8 on Windows

Vulnerability Insight
The flaw exists due to an improper sanitization used by VLC media player against MKV files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player MKV Files Arbitrary Code Execution Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.813579
Version used: 2023-07-20T05:05:18Z

References
cve: CVE-2018-11529
url: http://seclists.org/fulldisclosure/2018/Jul/28
cert-bund: CB-K18/0769
dfn-cert: DFN-CERT-2018-1427

High (CVSS: 7.8)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary
This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result
```
Fixed version:      Workaround
File checked:       C:\Windows\system32\IEXPRESS.EXE
File version:       11.0.19041.1
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution:
Solution type: Workaround
As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS
IExpress bundled with Microsoft Windows

Vulnerability Insight
The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method
Check for the presence of IExpress (IEXPRESS.EXE).
Details: `Windows IExpress Untrusted Search Path Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813808
Version used: `2023-07-20T05:05:18Z`

References
```
cve: CVE-2018-0598
url: http://jvn.jp/en/jp/JVN72748502/index.html
url: https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-
↪vulnerability
```

High (CVSS: 7.8)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary

. . . continues on next page . . .

... continued from previous page ...

This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result

```
Fixed version:      Workaround
File checked:       C:\Windows\system32\IEXPRESS.EXE
File version:       11.0.19041.1
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution:

Solution type: Workaround

As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS

IExpress bundled with Microsoft Windows

Vulnerability Insight

The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method

Check for the presence of IExpress (IEXPRESS.EXE).

Details: `Windows IExpress Untrusted Search Path Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.813808

Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-0598
url: http://jvn.jp/en/jp/JVN72748502/index.html
url: https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-
↪vulnerability
```

High (CVSS: 7.8)

NVT: VLC Media Player Subtitle Remote Code Execution Vulnerability (Windows)

Summary

VLC media player is prone to a heap overflow vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.7
```

... continues on next page ...

... continued from previous page ...

Fixed version: 2.2.5.1

Impact
Successful exploitation will allow remote attackers to take complete control over any device running them.

Solution:
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 2.2.5.1 or later.

Affected Software/OS
VideoLAN VLC media player before 2.2.5.1 on Windows.

Vulnerability Insight
The flaw exists due to the poor state of security in the way media player process subtitle files and the large number of subtitle formats. There are over 25 subtitle formats in use, each with unique features and capabilities. Media player often need to parse together multiple subtitle formats to ensure coverage and provide a better user experience. Like other, similar situations which involve fragmented software, this results in numerous distinct vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Subtitle Remote Code Execution Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.811052
Version used: 2023-07-14T16:09:27Z

References
cve: CVE-2017-8313
cve: CVE-2017-8312
cve: CVE-2017-8311
cve: CVE-2017-8310
url: http://blog.checkpoint.com/2017/05/23/hacked-in-translation
url: https://threatpost.com/subtitle-hack-leaves-200-million-vulnerable-to-remot
↪e-code-execution
cert-bund: CB-K17/1080
dfn-cert: DFN-CERT-2017-1113

High (CVSS: 7.8)
NVT: VLC Media Player < 3.0.9 DoS Vulnerability (Windows)

Summary
VLC Media Player is prone to a denial-of-service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7

... continues on next page ...

... continued from previous page ...

Fixed version: 3.0.9
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation would allow an attacker to trigger either a crash of VLC.

Solution:
Solution type: VendorFix
Update to version 3.0.9 or later.

Affected Software/OS
VideoLAN VLC Media Player before version 3.0.9 on Windows.

Vulnerability Insight
An off-by-one error in the DecodeBlock function in codec/sdl_image.c allows remote attackers to cause a denial-of-service (memory corruption) via a crafted image file.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player < 3.0.9 DoS Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.112755
Version used: 2021-07-22T11:01:40Z

References
cve: CVE-2019-19721
url: https://www.videolan.org/security/sb-vlc309.html
cert-bund: WID-SEC-2023-1517
cert-bund: CB-K20/0473
dfn-cert: DFN-CERT-2023-1422
dfn-cert: DFN-CERT-2020-0905

High (CVSS: 7.8)
NVT: VLC Media Player Multiple Vulnerabilities (sb-vlc308) - Windows

Summary
VLC Media Player is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 3.0.8
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to cause a denial of service condition and execute arbitrary code.

Solution:
Solution type: VendorFix
Update to version 3.0.8 or later.

Affected Software/OS
VLC Media Player versions prior to 3.0.8 on Windows.

Vulnerability Insight
The following flaws exist:
- Buffer overflow in the MKV demuxer
- Buffer overflow in the FAAD decoder
- Buffer overflow in the OGG demuxer
- Buffer overflow in the ASF demuxer
- A use after free in the MKV demuxer
- A use after free in the ASF demuxer
- Fix a couple of integer underflows in the MP4 demuxer
- A null dereference in the dvdnav demuxer
- A null dereference in the ASF demuxer
- A null dereference in the AVI demuxer
- A division by zero in the CAF demuxer
- A division by zero in the ASF demuxer

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player Multiple Vulnerabilities (sb-vlc308) - Windows`
OID:1.3.6.1.4.1.25623.1.0.815546
Version used: `2023-03-29T10:21:17Z`

References
`cve: CVE-2019-13602`
`cve: CVE-2019-14437`
`cve: CVE-2019-14438`
`cve: CVE-2019-14498`
`cve: CVE-2019-14533`
`cve: CVE-2019-14534`
`cve: CVE-2019-14535`
`cve: CVE-2019-14776`
`cve: CVE-2019-14777`
`cve: CVE-2019-14778`
`cve: CVE-2019-14970`
`url: https://www.videolan.org/security/sb-vlc308.html`
`cert-bund: CB-K19/0737`
`cert-bund: CB-K19/0609`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1753
dfn-cert: DFN-CERT-2019-1666
dfn-cert: DFN-CERT-2019-1534

High (CVSS: 7.8)
NVT: VLC Media Player Integer Underflow Vulnerability July19 (Windows)

Summary
VLC media player is prone to an integer underflow vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 3.0.8
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation will allow attackers to crash the application and launch further attacks using specially crafted files.

Solution:
Solution type: VendorFix
Update to version 3.0.8 or later.

Affected Software/OS
VideoLAN VLC media player prior to 3.0.8 on Windows.

Vulnerability Insight
The flaw exists due to an integer underflow issue in MP4_EIA608_Convert().

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Integer Underflow Vulnerability July19 (Windows)
OID:1.3.6.1.4.1.25623.1.0.815253
Version used: 2022-04-20T03:02:11Z

References
cve: CVE-2019-13602
url: https://www.videolan.org/security/sb-vlc308.html
url: https://git.videolan.org/?p=vlc.git;a=commit;h=8e8e0d72447f8378244f5b4a3dcd
↪e036dbeb1491
url: https://git.videolan.org/?p=vlc.git;a=commit;h=b2b157076d9e94df34502dd8df07
↪87deb940e938
cert-bund: CB-K19/0737
cert-bund: CB-K19/0609

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2019-1753
dfn-cert: DFN-CERT-2019-1666
dfn-cert: DFN-CERT-2019-1534

High (CVSS: 7.5)
NVT: Mozilla Firefox Security Updates(mfsa2022-13) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 97.0
Fixed version: 99
Installation
path / port: C:\Program Files\Mozilla Firefox

Impact
Successful exploitation will allow attackers to run arbitrary code, bypass security restrictions, conduct spoofing and cause a denial of service on affected system.

Solution:
Solution type: VendorFix
Upgrade to Mozilla Firefox version 99 or later, Please see the references for more information.

Affected Software/OS
Mozilla Firefox version before 99 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Use-after-free in NSSToken objects.
- Out of bounds write due to unexpected WebAuthN Extensions.
- Use-after-free in DocumentL10n::TranslateDocument.
- Missing security checks for fetching sourceMapURL.
- Script could be executed via svg's use element.
- Incorrect AliasSet used in JIT Codegen.
- iframe contents could be rendered outside the border.
- Text Selection could crash Firefox.
- Denial of Service via complex regular expressions.
- Memory safety bugs.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Mozilla Firefox Security Updates(mfsa2022-13) - Windows
OID:1.3.6.1.4.1.25623.1.0.821161
Version used: 2022-07-15T10:10:19Z

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2022-1097
cve: CVE-2022-28281
cve: CVE-2022-28282
cve: CVE-2022-28283
cve: CVE-2022-28284
cve: CVE-2022-28285
cve: CVE-2022-28286
cve: CVE-2022-28287
cve: CVE-2022-24713
cve: CVE-2022-28289
cve: CVE-2022-28288
url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-13
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0482
cert-bund: CB-K22/0396
dfn-cert: DFN-CERT-2023-0847
dfn-cert: DFN-CERT-2022-2557
dfn-cert: DFN-CERT-2022-1430
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0769
dfn-cert: DFN-CERT-2022-0763
dfn-cert: DFN-CERT-2022-0762
dfn-cert: DFN-CERT-2022-0553

High (CVSS: 7.5)
NVT: VLC Media Player M3U Denial of Service Vulnerability (Windows)

Summary
VLC Media Player is prone to denial of service and remote code execution vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Vulnerable range: Less than or equal to 2.0.8

Impact
Successful exploitation will allow attackers to cause denial of service and possibly execute arbitrary remote code.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.1.0 or later.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
VLC media player version 2.0.8 and prior on Windows

Vulnerability Insight
The flaw exists due to improper handling of a specially crafted M3U file.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player M3U Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.804125
Version used: `2022-04-25T14:50:49Z`

References
`cve: CVE-2013-6283`
`url: http://en.securitylab.ru/nvd/447008.php`
`url: http://www.securityfocus.com/bid/61844`
`url: http://www.exploit-db.com/exploits/27700`

[return to 10.0.0.5]

2.1.2 Medium general/tcp

Medium (CVSS: 6.9)
NVT: Adobe Reader Unspecified Vulnerability (Windows)

Summary
Adobe Reader is prone to an unspecified vulnerability.

Vulnerability Detection Result
`Installed version: 10.0.0`
`Vulnerable range:  10.0 - 10.1`

Impact
Successful exploitation will let attackers to gain privileges via unknown vectors.

Solution:
Solution type: VendorFix
Upgrade to Adobe Reader version 10.1.1 or later.

Affected Software/OS
Adobe Reader version 10.x through 10.1 on Windows

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

An unspecified flaw is present in the application which can be exploited through unknown attack vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Reader Unspecified Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.802165
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-1353`
`url: http://www.adobe.com/support/security/bulletins/apsb11-24.html`
`url: http://www.securityfocus.com/bid/49586`
`dfn-cert: DFN-CERT-2011-1784`
`dfn-cert: DFN-CERT-2011-1752`
`dfn-cert: DFN-CERT-2011-1750`
`dfn-cert: DFN-CERT-2011-1712`
`dfn-cert: DFN-CERT-2011-1419`

Medium (CVSS: 6.9)
NVT: Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)

Summary
A USB device driver software is prone to a code execution vulnerability.

Vulnerability Detection Result
`File checked for existence: C:\Windows\system32\hidserv.dll`

Impact
Successful exploitation will allow user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution:
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Checks via SMB if a specific device driver (hidserv.dll) exists on the target system.
Details: `Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Ja.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `2023-01-12T10:12:15Z`

References
`cve: CVE-2011-0638`
`url: http://www.cs.gmu.edu/~astavrou/publications.html`
`url: http://news.cnet.com/8301-27080_3-20028919-245.html`
`url: http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

Medium (CVSS: 6.9)
NVT: Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)

Summary
A USB device driver software is prone to a code execution vulnerability.

Vulnerability Detection Result
`File checked for existence: C:\Windows\system32\hidserv.dll`

Impact
Successful exploitation will allow user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution:
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Checks via SMB if a specific device driver (hidserv.dll) exists on the target system.
Details: `Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Ja.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `2023-01-12T10:12:15Z`

References
`cve: CVE-2011-0638`
`url: http://www.cs.gmu.edu/~astavrou/publications.html`
`url: http://news.cnet.com/8301-27080_3-20028919-245.html`
`url: http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

Medium (CVSS: 6.8)
NVT: Mozilla Firefox Security Update (MFSA2022-44) - Windows

Summary
Mozilla Firefox is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 97.0
Fixed version:     106
Installation
path / port:       C:\Program Files\Mozilla Firefox
```

Impact
Successful exploitation will allow attackers to run arbitrary code, cause denial of service and disclose sensitive information on an affected system.

Solution:
Solution type: VendorFix
Update to version 106 or later.

Affected Software/OS
Mozilla Firefox version before 106 on Windows.

Vulnerability Insight
Multiple flaws exist due to,
- Same-origin policy violation could have leaked cross-origin URLs.
- Memory Corruption in JS Engine.
- Denial of Service via window.print.

... continues on next page ...

... continued from previous page ...

- Race condition in DOM Workers.
- Username saved to a plaintext file on disk.
- Memory safety bugs.
- Memory corruption in WebGL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Mozilla Firefox Security Update (MFSA2022-44) - Windows`
OID:1.3.6.1.4.1.25623.1.0.826597
Version used: `2022-12-14T10:20:42Z`

References
`cve: CVE-2022-42927`
`cve: CVE-2022-42928`
`cve: CVE-2022-42929`
`cve: CVE-2022-42930`
`cve: CVE-2022-42931`
`cve: CVE-2022-42932`
`cve: CVE-2022-46881`
`cve: CVE-2022-46885`
`url: https://www.mozilla.org/en-US/security/advisories/mfsa2022-44`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2319`
`cert-bund: WID-SEC-2022-1791`
`dfn-cert: DFN-CERT-2023-0150`
`dfn-cert: DFN-CERT-2022-2836`
`dfn-cert: DFN-CERT-2022-2828`
`dfn-cert: DFN-CERT-2022-2551`
`dfn-cert: DFN-CERT-2022-2369`
`dfn-cert: DFN-CERT-2022-2301`

Medium (CVSS: 6.8)
NVT: VLC Media Player 'MP4_ReadBox_skcr()' Buffer Overflow Vulnerability - Windows

Summary
VLC Media Player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     1.1.9
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation could allow attackers to execute arbitrary code by tricking a user into opening a malicious file or visiting a specially crafted web page.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.9 or later.

Affected Software/OS
VLC media player version prior to 1.1.9 on Windows

Vulnerability Insight
The flaw is caused by a heap corruption error in the 'MP4_ReadBox_skcr()' [modules/demux/mp4/libmp4.c] function when processing malformed MP4 (MPEG-4 Part 14) data.

Vulnerability Detection Method
Details: `VLC Media Player 'MP4_ReadBox_skcr()' Buffer Overflow Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.801784
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-1684`
`url: http://secunia.com/advisories/44022`
`url: http://www.securityfocus.com/bid/47293`
`url: http://xforce.iss.net/xforce/xfdb/66664`
`url: http://www.vupen.com/english/advisories/2011/0916`

Medium (CVSS: 6.8)
NVT: VLC Media Player '.RM' File BOF Vulnerability (Windows)

Summary
VLC Media Player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     1.1.11
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation could allow attackers to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

Solution:
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.11 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
VLC media player version 1.1.0 to 1.1.10 on Windows.

Vulnerability Insight
The flaw is due to missing input validation when allocating memory using certain values from a RealAudio data block within RealMedia (RM) files.

Vulnerability Detection Method
Details: `VLC Media Player '.RM' File BOF Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.902704
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-2587`
`url: http://secunia.com/advisories/45066`
`url: http://www.securityfocus.com/bid/48664`
`url: http://xforce.iss.net/xforce/xfdb/68531`
`url: http://www.videolan.org/security/sa1105.html`

Medium (CVSS: 6.8)
NVT: VLC Media Player '.AVI' File BOF Vulnerability (Windows)

Summary
VLC Media Player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     1.1.11
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation could allow attackers to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

Solution:
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.11 or later.

Affected Software/OS
VLC media player version prior to 1.1.11 on Windows.

Vulnerability Insight
The flaw is due to an integer underflow error when parsing the 'strf' chunk within AVI files can be exploited to cause a heap-based buffer overflow.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: VLC Media Player '.AVI' File BOF Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.902705
Version used: 2022-04-28T13:38:57Z

References
cve: CVE-2011-2588
url: http://secunia.com/advisories/45066
url: http://www.securityfocus.com/bid/48664
url: http://xforce.iss.net/xforce/xfdb/68532
url: http://www.videolan.org/security/sa1106.html

Medium (CVSS: 6.8)
NVT: VLC Media Player OGG Demuxer Buffer Overflow Vulnerability (Windows)

Summary
VLC Media Player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.0.2
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation could allow attackers to execute arbitrary code on the target system.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.2 or later.

Affected Software/OS
VLC media player versions prior to 2.0.2 on Windows

Vulnerability Insight
A boundary error exists within the 'Ogg_DecodePacket()' function (modules/demux/ogg.c) when processing OGG container files. This can be exploited to cause heap-based buffer overflow via a specially crafted OGG file.

Vulnerability Detection Method
Details: VLC Media Player OGG Demuxer Buffer Overflow Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.802922
Version used: 2022-04-27T12:01:52Z

... continues on next page ...

... continued from previous page ...

References
cve: CVE-2012-3377
url: http://secunia.com/advisories/49835
url: http://www.securityfocus.com/bid/54345
url: http://xforce.iss.net/xforce/xfdb/76800
url: http://www.securitytracker.com/id?1027224
url: http://www.openwall.com/lists/oss-security/2012/07/06/1
url: http://www.openwall.com/lists/oss-security/2012/07/06/2
url: http://git.videolan.org/?p=vlc/vlc-2.0.git;a=commitdiff;h=16e9e126333fb7acb
↪47d363366fee3deadc8331e

Medium (CVSS: 6.8)
NVT: VLC Media Player mp4a Denial of Service Vulnerability (Windows)

Summary
VLC Media Player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Vulnerable range: Less than or equal to 2.0.7

Impact
Successful exploitation will allow attackers to overflow buffer, cause denial of service.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.8 or later.

Affected Software/OS
VLC media player version 2.0.7 and prior on Windows.

Vulnerability Insight
A flaw exists in mpeg4audio.c file, which to perform adequate boundary checks on user-supplied input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player mp4a Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803954
Version used: 2022-04-25T14:50:49Z

References
cve: CVE-2013-4388
url: http://www.securitytracker.com/id/1029120
url: http://www.securityfocus.com/bid/62724

... continues on next page ...

... continued from previous page ...

url: http://www.openwall.com/lists/oss-security/2013/10/01/2
cert-bund: CB-K14/0835
cert-bund: CB-K13/0778
dfn-cert: DFN-CERT-2014-0871

Medium (CVSS: 6.8)
NVT: VLC Media Player Buffer Overflow Vulnerability - July 13 (Windows)

Summary
VLC Media Player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.0.6
Installation
path / port: C:\Program Files (x86)\VideoLAN\VLC

Impact
Successful exploitation could allow attackers to execute arbitrary code or cause denial of service condition in the context of affected application via crafted ASF file.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.6 or later.

Affected Software/OS
VLC media player version 2.0.5 and prior on Windows

Vulnerability Insight
Flaw due to error in 'DemuxPacket()' function in the ASF Demuxer component (modules/demux/asf/asf.c) when parsing ASF files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Buffer Overflow Vulnerability - July 13 (Windows)
OID:1.3.6.1.4.1.25623.1.0.803698
Version used: 2022-04-25T14:50:49Z

References
cve: CVE-2013-1954
url: http://secunia.com/advisories/51995
url: http://www.securityfocus.com/bid/57333
url: http://www.videolan.org/security/sa1302.html
cert-bund: CB-K14/0835
dfn-cert: DFN-CERT-2014-0871

Medium (CVSS: 6.8)
NVT: VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Windows)

Summary
VLC media player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 1.1.7`
`Fixed version: 2.2.2`

Impact
Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted 3GP file.

Solution:
Solution type: VendorFix
Updates are available, please see the references for more information.

Affected Software/OS
VideoLAN VLC media player 2.2.1 and earlier on Windows.

Vulnerability Insight
The flaw is due to insufficient restrictions on a writable buffer which affects the 3GP file format parser.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.806086
Version used: `2022-04-14T06:42:08Z`

References
`cve: CVE-2015-5949`
`url: https://packetstormsecurity.com/files/133266`
`url: http://www.securityfocus.com/bid/76448`
`url: http://www.securityfocus.com/archive/1/archive/1/536287/100/0/threaded`
`cert-bund: CB-K15/1242`
`dfn-cert: DFN-CERT-2015-1307`

Medium (CVSS: 6.8)
NVT: VLC Media Player 'AMV' Denial of Service Vulnerability (Windows)

Summary
VLC Media Player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 1.1.7
Fixed version:     1.1.10
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation could allow attackers to cause a denial of service or possibly execute arbitrary code via a malformed AMV file.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 1.1.10 or later.

Affected Software/OS
VLC media player version 1.1.9 and prior on Windows.

Vulnerability Insight
The flaw is due to error while handling 'sp5xdec.c' in the Sunplus SP5X JPEG decoder in libavcodec, performs a write operation outside the bounds of an unspecified array.

Vulnerability Detection Method
Details: `VLC Media Player 'AMV' Denial of Service Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.802119
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-1931`
`url: http://www.securityfocus.com/archive/1/517706`
`url: http://www.securityfocus.com/bid/47602`
`url: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=624339`

Medium (CVSS: 5.5)
NVT: VLC Media Player 'libebml' Library Heap Overflow Vulnerability July19 (Windows)

Summary
VLC Media Player is prone to a heap-based buffer over-read vulnerability.

Vulnerability Detection Result

```
Installed version: 1.1.7
Fixed version:     3.0.3
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to cause denial of service condition and launch further attacks using specially crafted files.

Solution:
Solution type: VendorFix
Update VLC Media Player to version 3.0.3 or later.

Affected Software/OS
libebml before 1.3.6, as used in the MKV module in VLC Media Player binaries before 3.0.3 on Windows.

Vulnerability Insight
The flaw exists due to a heap-based buffer over-read error in EbmlElement::FindNextElement of the 'libebml' library as used by VLC Media Player.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player 'libebml' Library Heap Overflow Vulnerability July19 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.815255
Version used: `2022-04-13T07:21:45Z`

References
`cve: CVE-2019-13615`
`url: https://trac.videolan.org/vlc/ticket/22474`
`url: http://www.securityfocus.com/bid/109304`
`url: https://github.com/Matroska-Org/libebml/commit/05beb69ba60acce09f73ed491bb7`
`↪6f332849c3a0`
`url: https://github.com/Matroska-Org/libebml/commit/b66ca475be967547af9a3784e720`
`↪fbbacd381be6`
`url: https://github.com/Matroska-Org/libebml/compare/release-1.3.5...release-1.3`
`↪.6`
`cert-bund: CB-K19/0634`
`dfn-cert: DFN-CERT-2019-1533`

Medium (CVSS: 5.5)
NVT: VLC Media Player Denial of Service Vulnerability April-16 (Windows)

Summary
VLC media player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
`Installed version: 1.1.7`
`Fixed version: 2.2.0`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted wav file.

Solution:
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 2.2.0 or later.

Affected Software/OS
VideoLAN VLC media player before 2.2.0 on Windows.

Vulnerability Insight
The flaw is due to the buffer overflow in the 'AStreamPeekStream' function in 'input/stream.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player Denial of Service Vulnerability April-16 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.807929
Version used: `2023-07-21T05:05:22Z`

References
`cve: CVE-2016-3941`
`url: http://www.securitytracker.com/id/1035456`
`url: https://bugs.launchpad.net/ubuntu/+source/vlc/+bug/1533633`
`cert-bund: CB-K16/0963`
`dfn-cert: DFN-CERT-2016-1016`

Medium (CVSS: 4.4)
NVT: VLC Media Player Buffer Overflow Vulnerability Oct16

Summary
VLC media player is prone to a buffer overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     2.2.4
```

Impact
Successful exploitation will allow local attackers to cause denial of service condition.

Solution:
Solution type: VendorFix
Update to version 2.2.4.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
VideoLAN VLC media player 2.2.3 on Windows.

Vulnerability Insight
The flaw is due to an insufficient validation of user supplied input while opening a file in player.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `VLC Media Player Buffer Overflow Vulnerability Oct16`
OID:1.3.6.1.4.1.25623.1.0.807370
Version used: `2023-07-20T05:05:17Z`

References
`url: https://www.exploit-db.com/exploits/40439`
`url: https://www.videolan.org/security/sa1601.html`

Medium (CVSS: 4.3)
NVT: Adobe Products Unspecified Cross-Site Scripting Vulnerability June-2011 (Windows)

Summary
Adobe Flash Player, Adobe Reader or Acrobat is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 10.0.0
Vulnerable range:  Less than or equal to 10.0.3
Installation
path / port:       C:\Program Files (x86)\Adobe\Reader 10.0\Reader\
```

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.

Solution:
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.3.181.22 or later.

Affected Software/OS
Adobe Flash Player versions prior to 10.3.181.22 on Windows.
Adobe Reader and Acrobat X versions 10.0.3 and prior on Windows.

Vulnerability Insight
The flaw is caused by improper validation of certain unspecified input, which allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Adobe Products Unspecified Cross-Site Scripting Vulnerability June-2011 (Window.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802206
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2011-2107`
`url: http://www.adobe.com/support/security/bulletins/apsb11-13.html`
`url: http://www.securityfocus.com/bid/48107`
`dfn-cert: DFN-CERT-2011-1677`
`dfn-cert: DFN-CERT-2011-0921`
`dfn-cert: DFN-CERT-2011-0883`
`dfn-cert: DFN-CERT-2011-0880`

Medium (CVSS: 4.3)
NVT: VLC Media Player 'libpng_plugin' Denial of Service Vulnerability (Windows)

Summary
VLC Media Player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.1.7
Fixed version:     2.0.4
Installation
path / port:       C:\Program Files (x86)\VideoLAN\VLC
```

Impact
Successful exploitation will allow attackers to crash the affected application and denying service to legitimate users.

Solution:
Solution type: VendorFix
Upgrade to VLC media player 2.0.4 or later.

Affected Software/OS
VLC media player version 2.0.3 and prior on Windows

Vulnerability Insight
The flaw is due to an error in 'libpng_plugin' when handling a crafted PNG file. Which can be exploited to cause a crash.

Vulnerability Detection Method
Details: `VLC Media Player 'libpng_plugin' Denial of Service Vulnerability (Windows)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.802488
Version used: 2022-04-27T12:01:52Z

References
cve: CVE-2012-5470
url: http://www.exploit-db.com/exploits/21889/
url: http://www.securityfocus.com/bid/55850
url: http://www.videolan.org/vlc/releases/2.0.4.html
url: http://openwall.com/lists/oss-security/2012/10/24/3

Medium (CVSS: 4.3)
NVT: VLC Media Player ASF Demuxer Denial of Service Vulnerability (Windows)

Summary
VLC Media Player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Vulnerable range: Less than or equal to 2.1.2

Impact
Successful exploitation will allow attackers to cause a denial of service condition.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.1.3 or later.

Affected Software/OS
VLC media player version 2.1.2 and prior on Windows.

Vulnerability Insight
The flaw exists due to a divide-by-zero error when processing malicious '.asf' files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player ASF Demuxer Denial of Service Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.804323
Version used: 2022-04-14T11:24:11Z

References
cve: CVE-2014-1684
url: http://xforce.iss.net/xforce/xfdb/90955
url: http://www.securityfocus.com/bid/65399
url: http://www.exploit-db.com/exploits/31429
url: http://www.videolan.org/developers/vlc-branch/NEWS

... continues on next page ...

... continued from previous page ...

url: http://packetstormsecurity.com/files/125080/VLC-Media-Player-2.1.2-Denial-O
↪f-Service.html

Medium (CVSS: 4.3)
NVT: VLC Media Player Denial of Service Vulnerability Mar14 (Windows)

Summary
VLC Media Player is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 1.1.7
Fixed version: 2.0.7

Impact
Successful exploitation will allow attackers to cause a denial of service conditions.

Solution:
Solution type: VendorFix
Upgrade to VLC media player version 2.0.7 or later.

Affected Software/OS
VLC media player version 2.0.6 and prior on Windows.

Vulnerability Insight
The flaw exists due to some unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: VLC Media Player Denial of Service Vulnerability Mar14 (Windows)
OID:1.3.6.1.4.1.25623.1.0.804346
Version used: 2021-10-28T14:26:49Z

References
cve: CVE-2013-7340
url: http://www.videolan.org/developers/vlc-branch/NEWS
cert-bund: CB-K14/0349
dfn-cert: DFN-CERT-2014-0361

[return to 10.0.0.5]

2.1.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49667]
Port: 49668/tcp
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49668]
Port: 49669/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
```

... continues on next page ...

... continued from previous page ...

```
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
Port: 49670/tcp
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49670]
      Annotation: Remote Fw APIs
Port: 49673/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:10.0.0.5[49673]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[return to 10.0.0.5]

2.1.4 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
```

... continues on next page ...

... continued from previous page ...

↪.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 10.0.0.5]

2.1.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.0.5]

This file was automatically generated.