

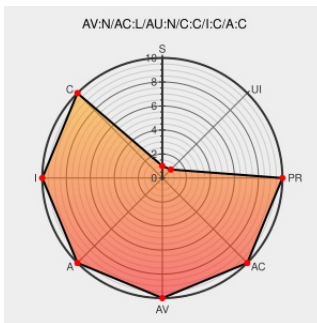


CVE-2014-1551

Published on: 07/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-1551

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

Use-after-free vulnerability in the FontTableRec destructor in Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 on Windows allows remote attackers to execute arbitrary code via crafted use of fonts in MathML content, leading to improper handling of a DirectWrite font-face object.

CVE-2014-1551 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[www.oracle.com](#)
[text/html](#)

CONFIRM
www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html

Gentoo Security

[security.gentoo.org](#)
[text/html](#)

GENTOO GLSA-201504-01

Security Advisory SA59760 - Waterfox Firefox
Multiple Vulnerabilities - Secunia

[web.archive.org](#)
[text/html](#)

SECUNIA 59760

MFSa 2014-59: Use-after-free in DirectWrite font
handling

[Vendor Advisory](#)
[www.mozilla.org](#)
[text/html](#)

CONFIRM
www.mozilla.org/security/announce/2014/mfsa2014-59.html

Mozilla Thunderbird Multiple Flaws Let Remote
Attackers Execute Arbitrary Code

[www.securitytracker.com](#)

SECTrack 1030620

Users Deny Service and Execute Arbitrary Code - SecurityTracker	text/html	
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Spoof User Interface Elements - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1030619
Access Denied	bugzilla.mozilla.org text/html	 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1018234

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	24.0	All	All	All
Application	Mozilla	Firefox Esr	24.0.1	All	All	All
Application	Mozilla	Firefox Esr	24.0.2	All	All	All
Application	Mozilla	Firefox Esr	24.1.0	All	All	All
Application	Mozilla	Firefox Esr	24.1.1	All	All	All
Application	Mozilla	Firefox Esr	24.2	All	All	All
Application	Mozilla	Firefox Esr	24.3	All	All	All
Application	Mozilla	Firefox Esr	24.4	All	All	All
Application	Mozilla	Firefox Esr	24.5	All	All	All
Application	Mozilla	Firefox Esr	24.6	All	All	All
Application	Mozilla	Firefox Esr	24.0	All	All	All
Application	Mozilla	Firefox Esr	24.0.1	All	All	All
Application	Mozilla	Firefox Esr	24.0.2	All	All	All
Application	Mozilla	Firefox Esr	24.1.0	All	All	All
Application	Mozilla	Firefox Esr	24.1.1	All	All	All
Application	Mozilla	Firefox Esr	24.2	All	All	All
Application	Mozilla	Firefox Esr	24.3	All	All	All
Application	Mozilla	Firefox Esr	24.4	All	All	All
Application	Mozilla	Firefox Esr	24.5	All	All	All

Application	Mozilla	Firefox Esr	24.6	All	All	All
Application	Mozilla	Thunderbird	24.0	All	All	All
Application	Mozilla	Thunderbird	24.0.1	All	All	All
Application	Mozilla	Thunderbird	24.1	All	All	All
Application	Mozilla	Thunderbird	24.1.1	All	All	All
Application	Mozilla	Thunderbird	24.2	All	All	All
Application	Mozilla	Thunderbird	24.3	All	All	All
Application	Mozilla	Thunderbird	24.4	All	All	All
Application	Mozilla	Thunderbird	24.5	All	All	All
Application	Mozilla	Thunderbird	24.0	All	All	All
Application	Mozilla	Thunderbird	24.0.1	All	All	All
Application	Mozilla	Thunderbird	24.1	All	All	All
Application	Mozilla	Thunderbird	24.1.1	All	All	All
Application	Mozilla	Thunderbird	24.2	All	All	All
Application	Mozilla	Thunderbird	24.3	All	All	All
Application	Mozilla	Thunderbird	24.4	All	All	All
Application	Mozilla	Thunderbird	24.5	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
cpe:2.3:o:microsoft:windows:*.***.***.***:						
cpe:2.3:o:microsoft:windows:***.***.***.***:						
cpe:2.3:a:mozilla:firefox:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.0:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.0.1:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.0.2:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.1.0:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.1.1:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.2:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.3:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.4:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.5:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.6:***.***.***.***:						
cpe:2.3:a:mozilla:firefox_esr:24.0:***.***.***.***:						

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)