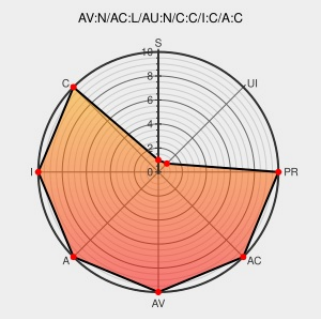
CVE-2014-1550

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

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1550

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

Use-after-free vulnerability in the MediaInputPort class in Mozilla Firefox before 31.0 and Thunderbird before 31.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging incorrect Web Audio control-message ordering.

CVE-2014-1550 has been assigned by security@mozilla.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisory SA60628 - SUSE update for MozillaFirefox - Secunia	web.archive.org text/html	SECUNIA 60628
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
Mozilla Thunderbird Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code -	www.securitytracker.com text/html	SECTRACK 1030620

Security Tracker		
MFSA 2014-58: Use-after-free in Web Audio due to incorrect control message ordering	Vendor Advisory www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2014/mfsa2014-58.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=1020411

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	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	24.6	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	24.6	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:24.0:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.0.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.1.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.2:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.3:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.4:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.5:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.0:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.0.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.1.1:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.2:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.3:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.4:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.5:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:24.6:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→