CVE-2015-0813

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-0813
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-01 10:59:00 UTC
Updated	2017-01-03 02:59:00 UTC
Description	Use-after-free vulnerability in the AppendElements function in Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, an

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References

Reference
Debian -- Security Information -- DSA-3212-1 icedove
[security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox
Access Denied
[security-announce] openSUSE-SU-2015:0892-1: important: Update to Firefo
Use-after-free when using the Fluendo MP3 GStreamer plugin — Mozilla
[security-announce] SUSE-SU-2015:0704-1: important: Security update for
Mozilla Thunderbird Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Request Forgery Attacks - SecurityTracker
USN-2550-1: Firefox vulnerabilities | Ubuntu
Red Hat Customer Portal

Mozilla Firefox/Thunderbird CVE-2015-0813 Use After Free Memory Corruption Vulnerability
Mozilla Firefox Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - S
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security
USN-2552-1: Thunderbird vulnerabilities | Ubuntu
Debian -- Security Information -- DSA-3211-1 iceweasel
Oracle Solaris Third Party Bulletin - April 2015
[security-announce] openSUSE-SU-2015:0677-1: important: Security update
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**