CVE-2015-2713

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

Summary

CVE	CVE-2015-2713
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-14 10:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in the SetBreaks function in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thun

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	31.0	All	All	All

Application	Mozilla	Firefox	31.1.0	All	All	All
Application	Mozilla	Firefox	31.1.1	All	All	All
Application	Mozilla	Firefox	31.3.0	All	All	All
Application	Mozilla	Firefox	31.5.1	All	All	All
Application	Mozilla	Firefox	31.5.2	All	All	All
Application	Mozilla	Firefox	31.5.3	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	31.1	All	All	All
Application	Mozilla	Firefox Esr	31.2	All	All	All
Application	Mozilla	Firefox Esr	31.3	All	All	All
Application	Mozilla	Firefox Esr	31.4	All	All	All
Application	Mozilla	Firefox Esr	31.5	All	All	All
Application	Mozilla	Firefox Esr	31.6.0	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Access Denied	af854a3a-2127-422b-91ae-364da2661108	bugzilla.mo
[security-announce] SUSE-SU-2015:0960-1: important: Security update for	af854a3a-2127-422b-91ae-364da2661108	lists.opens
openSUSE-SU-2015:0934-1: moderate: Security update for MozillaFirefox	af854a3a-2127-422b-91ae-364da2661108	lists.opens
Security Advisories for Thunderbird — Mozilla	af854a3a-2127-422b-91ae-364da2661108	www.mozil
Use-after-free during text processing with vertical text enabled — Mozilla	af854a3a-2127-422b-91ae-364da2661108	www.mozil
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.
USN-2602-1: Firefox vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubunt
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	security.ge
Mozilla Firefox and Thunderbird MFSA 2015-48 through -58 Multiple Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.secur
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.
USN-2603-1: Thunderbird vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubunt

USN-2803-1: Thunderbird vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubun
Debian -- Security Information -- DSA-3260-1 iceweasel	af854a3a-2127-422b-91ae-364da2661108	www.debia
Debian -- Security Information -- DSA-3264-1 icedove	af854a3a-2127-422b-91ae-364da2661108	www.debia
[security-announce] SUSE-SU-2015:0978-1: important: Security update for	af854a3a-2127-422b-91ae-364da2661108	lists.opens
[security-announce] openSUSE-SU-2015:0892-1: important: Update to Firefo	af854a3a-2127-422b-91ae-364da2661108	lists.opens
[security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox	af854a3a-2127-422b-91ae-364da2661108	lists.opens
Oracle Solaris Bulletin - April 2016	af854a3a-2127-422b-91ae-364da2661108	www.oracl
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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**