CVE-2012-4201

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

Summary

CVE	CVE-2012-4201
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-21 12:55:00 UTC
Updated	2020-08-14 17:33:00 UTC
Description	The evalInSandbox implementation in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All

Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All

References

Reference	Source	Link
MFSA 2012-93: evalInSanbox location context incorrectly applied	CONFIRM	www.mozilla.org
Security Advisory SA51440 - SUSE update for seamonkey - Secunia	SECUNIA	secunia.com
Security Advisory SA51359 - Red Hat update for firefox - Secunia	SECUNIA	secunia.com
Security Advisory SA51434 - SUSE update for xulrunner - Secunia	SECUNIA	secunia.com
87594	OSVDB	osvdb.org
Debian -- Security Information -- DSA-2588-1 icedove	DEBIAN	www.debian.org
Mozilla Firefox, SeaMonkey, and Thunderbird CVE-2012-4201 Cross Site Scripting Vulnerability	BID	www.securityfocus.com
openSUSE-SU-2012:1583-1: moderate: update for MozillaFirefox	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
openSUSE-SU-2012:1585-1: moderate: update for MozillaThunderbird	SUSE	lists.opensuse.org
USN-1636-1: Thunderbird vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
Debian -- Security Information -- DSA-2583-1 iceweasel	DEBIAN	www.debian.org
USN-1638-2: ubufox update | Ubuntu	UBUNTU	www.ubuntu.com
Security Advisory SA51360 - Red Hat update for thunderbird - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
USN-1638-1: Firefox vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
About Secunia Research | Flexera	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.co
Support / Security / Advisories / / MDVSA-2012:173 | Mandriva	MANDRIVA	www.mandriva.com
[security-announce] SUSE-SU-2012:1592-1: important: Security update for	SUSE	lists.opensuse.org
USN-1638-3: Firefox regressions | Ubuntu	UBUNTU	www.ubuntu.com
747607 – (CVE-2012-4201) Problem with evalInSandbox and location	CONFIRM	bugzilla.mozilla.org
[security-announce] openSUSE-SU-2013:0175-1: important: security update	SUSE	lists.opensuse.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
Security Advisory SA51369 - Ubuntu update for firefox - Secunia	SECUNIA	secunia.com
Security Advisory SA51370 - Ubuntu update for thunderbird - Secunia	SECUNIA	secunia.com
openSUSE-SU-2012:1586-1: moderate: update for xulrunner	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-2584-1 iceape	DEBIAN	www.debian.org
Security Advisory SA51439 - SUSE update for MozillaFirefox - Secunia	SECUNIA	secunia.com

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**