CVE-2012-0444

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

Summary

CVE	CVE-2012-0444
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-02-01 16:55:00 UTC
Updated	2020-08-28 13:12:00 UTC
Description	Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2

Risk And Classification

Problem Types: CWE-119

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	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	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
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp1	All	All

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisecurity.org
Support / Security / Advisories / / MDVSA-2012:013 | Mandriva	MANDRIVA	www.mandriva.com
IBM X-Force Exchange	XF	exchange.xforce.ibmc
[security-announce] openSUSE-SU-2012:0234-1: important: MozillaFirefox:	SUSE	lists.opensuse.org
Security Advisory SA48095 - Ubuntu update for libvorbis - Secunia	SECUNIA	secunia.com
MFSA 2012-07: Potential Memory Corruption When Decoding Ogg Vorbis files	CONFIRM	www.mozilla.org
Debian -- Security Information -- DSA-2406-1 icedove	DEBIAN	www.debian.org
Security Advisory SA48043 - Debian update for libvorbis - Secunia	SECUNIA	secunia.com
Mozilla Firefox/Thunderbird/SeaMonkey Ogg Vorbis Files Memory Corruption Vulnerability	BID	www.securityfocus.co
[security-announce] SUSE-SU-2012:0198-1: important: Security update for	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-2400-1 iceweasel	DEBIAN	www.debian.org
Debian -- Security Information -- DSA-2402-1 iceape	DEBIAN	www.debian.org
USN-1370-1: libvorbis vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
719612 – (CVE-2012-0444) Mozilla Firefox Ogg Vorbis Decoding Memory Corruption (ZDI-CAN-1477)	CONFIRM	bugzilla.mozilla.org
[security-announce] SUSE-SU-2012:0221-1: important: Security update for	SUSE	lists.opensuse.org

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**