CVE-2011-3905

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-3905
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-12-13 21:55:00 UTC
Updated	2023-11-07 02:08:00 UTC
Description	libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	7.0	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	7.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference	Source	Link
Chrome Releases: Stable Channel Update	CONFIRM	googlechromereleases.blogspot.com
Support / Security / Advisories / / MDVSA-2011:188 | Mandriva	MANDRIVA	www.mandriva.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Debian -- Security Information -- DSA-2394-1 libxml2	DEBIAN	www.debian.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
95465 - chromium - An open-source project to help move the web forward. - Monorail	CONFIRM	code.google.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.