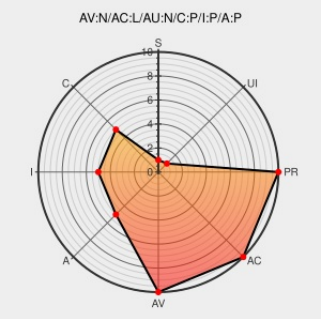
CVE-2011-2821

Published on: 08/29/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:20 PM UTC

CVE-2011-2821

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Iphone Os from Apple contain the following vulnerability:

Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.

CVE-2011-2821 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Support	Third Party Advisory, www.redhat.com, text/html	REDHAT RHSA-2011:1749
Chrome Releases: Stable Channel Update	Vendor Advisory, googlechromereleases.blogspot.com, text/html	CONFIRM googlechromereleases.blogspot.com/2011/08/stable-channel-update_22.html
HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Unauthorized Access, Disclosure of Information, Data Modification, Denial of Service (DoS), Execution of Arbitrary Code - c03360041 - HP Business Support Center	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	HP SSRT100877
Red Hat Customer Portal	Third Party Advisory	REDHAT RHSA-2013:0217

	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	RED HAT RHSA 2013:0217
APPLE-SA-2012-09-19-1 iOS 6	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2012-09-19-1
About the security content of OS X Lion v10.7.4 and Security Update 2012-002	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT5281
APPLE-SA-2012-05-09-1 OS X Lion v10.7.4 and Security Update 2012-002	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2012-05-09-1
Debian -- Security Information -- DSA-2394-1 libxml2	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2394
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:13840
Support / Security / Advisories / / MDVSA-2011:145 | Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2011:145
Issue 89402 - chromium - Memory corruption (double free) caused by malformed XPath expression in XSLT - An open-source browser project to help move the web forward. - Google Project Hosting	Exploit Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=89402
About the security content of iOS 6	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT5503

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	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
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 Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	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 Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→