



CVE-2011-2834

Published on: 09/17/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:21 PM UTC

CVE-2011-2834

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 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.

CVE-2011-2834 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Support

Third Party Advisory
www.redhat.com
text/html

[REDHAT RHSA-2011:1749](#)

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](#)

Chrome Releases: Stable Channel Update

Vendor Advisory
googlechromereleases.blogspot.com
text/html

CONFIRM
googlechromereleases.blogspot.com/2011/09/stable-channel-update_16.html

Red Hat Customer Portal

Third Party Advisory

[REDHAT RHSA-2013:0217](#)

Third Party Advisory	web.archive.org	text/html	Inactive Link	Not Archived	
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	Deprecated Link	text/html	DEBIAN DSA-2394
Google Project Hosting	Exploit	Issue Tracking	Patch	Vendor Advisory	code.google.com/p/chromium/issues/detail?id=93472
IBM X-Force Exchange	Third Party Advisory	VDB Entry	exchange.xforce.ibmcloud.com	text/html	XF chrome-libxml-code-execution(69885)
Support / Security / Advisories // MDVSA-2011:145 Mandriva	Third Party Advisory	www.mandriva.com	text/html		MANDRIVA MDVSA-2011:145
No Description Provided	Broken Link	osvdb.org	Inactive Link	Not Archived	OSVDB 75560
Repository / Oval Repository	Third Party Advisory	oval.cisecurity.org	text/html		OVAL oval.org.mitre.oval:def:14410
About the security content of iOS 6	Third Party Advisory	support.apple.com	text/html		CONFIRM support.apple.com/kb/HT5503

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 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
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_server:6.0:****:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:****:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.3:****:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.3:****:*:*:
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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)