CVE-2011-3046

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

Summary

CVE	CVE-2011-3046
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-09 00:55:00 UTC
Updated	2020-04-16 15:59:00 UTC
Description	The extension subsystem in Google Chrome before 17.0.963.78 does not properly handle history navigation, which allows r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All

References

Reference
Chrome Releases: Chrome Stable Channel Update
Sundar Pichai - Google+ - Congrats to long-time Chromium contributor Sergey Glazunov…
Google Chrome Unspecified Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker
Google Chrome Prior to 17.0.963.78 Multiple Security Vulnerabilities
About Secunia Research | Flexera
Security Alerts - Secunia

Security Alerts - Secunia
117226 - chromium - An open-source project to help move the web forward. - Monorail
APPLE-SA-2012-05-07-1 iOS 5.1.1 Software Update
Repository / Oval Repository
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities
APPLE-SA-2012-05-09-2 Safari 5.1.7
[security-announce] openSUSE-SU-2012:0374-1: important: update for chrom
Issue 117230 - chromium - Part 2 of Pwnium Bug - An open-source browser project to help move the web forward. - Google Project Hosting
About the security content of Safari 5.1.7
About Secunia Research | Flexera
CanSecWest Pwnium: Google Chrome hacked with sandbox bypass | ZDNet
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
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 registred 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**