



CVE-2015-1211

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-1211
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-06 11:59:00 UTC
Updated	2023-11-07 02:24:00 UTC
Description	The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	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	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	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 Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	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
USN-2495-1: Oxide vulnerabilities Ubuntu	UBUNTU
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code and Bypass Same-Origin Restrictions - SecurityTracker	SECTRA
Security Advisory SA62818 - Google Chrome for Android Multiple Vulnerabilities - Secunia	SECUNIA
Security Advisory SA62917 - Red Hat update for chromium-browser - Secunia	SECUNIA
Issue 889323002: Allow SW registration only if it's secure AND it's HTTP or HTTPS - Code Review	
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities	GENTOO
Inicio de sesión - Cuentas de Google	CONFIRM
Chrome Releases: Stable Channel Update	
Google Chrome Prior to 40.0.2214.109 Multiple Security Vulnerabilities	
Security Advisory SA62925 - Ubuntu update for oxide-qt - Secunia	SECUNIA
[security-announce] openSUSE-SU-2015:0441-1: important: Security update	SUSE
IBM X-Force Exchange	
Security Advisory SA62670 - Google Chrome Multiple Vulnerabilities - Secunia	
Red Hat Customer Portal	
Chrome Releases: Chrome for Android Update	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 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](#).

Free CVE JSON API [cve.report/api](#)

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