



CVE-2015-6792

Published on: 12/23/2015 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:27:00 AM UTC

CVE-2015-6792

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.

CVE-2015-6792 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Google Chrome Bugs Let Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRAK 1034491

Google Chrome Prior to 47.0.2526.106 Multiple Remote Code Execution Vulnerabilities	cve.report (archive) text/html	 BID 79348
Issue 1500153002: Fix crash with MIDI send for MidiManagerAlsa - Code Review	codereview.chromium.org text/html	 CONFIRM codereview.chromium.org/1500153002
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201603-09
Issue 569486 - chromium - Tracking bug for internal fixes: Chrome M47, Release 2 - ???? ** Chromium issue tracking will soon migrate to https://bugs.chromium.org (Monorail) ** ???? - Google Project Hosting	code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=569486
Debian -- Security Information -- DSA-3456-1 chromium-browser	www.debian.org text/html Deprecated Link	 DEBIAN DSA-3456
Issue 564501 - chromium - Security: UAF in MidiHost (Sandbox escape) - Monorail	code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=564501
Issue 1508563003: Fix a potential crash in MidiManagerMac. - Code Review	codereview.chromium.org text/html	 CONFIRM codereview.chromium.org/1508563003
[security-announce] openSUSE-SU-2015:2347-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2347
Chrome Releases: Stable Channel Update	googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2015/12/stable-channel-update_15.html
[security-announce] openSUSE-SU-2015:2346-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2346
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:2665

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
Application	Google	Chrome	All	All	All	All
<code>cpe:2.3:a:google:chrome:*:*:*:*:*.*</code>						

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](#)