



CVE-2015-6783

Published on: 12/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6783

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The FindStartOffsetOfFileInZipFile function in crazy_linker_zip.cpp in crazy_linker (aka Crazy Linker) in Android 5.x and 6.x, as used in Google Chrome before 47.0.2526.73, improperly searches for an EOCD record, which allows attackers to bypass a signature-validation requirement via a crafted ZIP archive.

CVE-2015-6783 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

[security-announce] openSUSE-SU-2015:2291-1: important: Security update

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2015:2291](#)

Chrome Releases: Stable Channel Update

[Vendor Advisory](#)
[googlechromereleases.blogspot.com](#)
[text/html](#)

[CONFIRM googlechromereleases.blogspot.com/20](#)

d9e316238aee59acf665d80b544cf4e1edfd3349 - chromium/src.git - Git at Google

[chromium.googlesource.com](#)
[text/html](#)

[CONFIRM chromium.googlesource.com/chromium/src.git/+d9e31](#)

Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Spoof Content - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1034298](#)

Google Chrome Prior to 47.0.2526.73 Multiple Security Vulnerabilities	cve.report (archive) text/html	 BID /8416
Issue 537205 - chromium - Security: Crazy Linker on Android allows modification of Chrome APK without breaking signature - ???? ** 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=537205
Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201603-09
[security-announce] openSUSE-SU-2015:2290-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2290

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	Google	Android	5.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All

cpe:2.3:o:google:android:5.0:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:

cpe:2.3:o:google:android:5.0:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

© [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](#)