

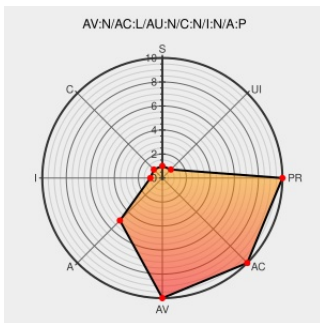


CVE-2015-1246

Published on: 04/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1246

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

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2015-1246 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-3238-1 chromium-browser

www.debian.org
Deprecated Link
text/html

[DEBIAN DSA-3238](#)

Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Same-Origin Restrictions - SecurityTracker

www.securitytracker.com
text/html

[SECTRAK 1032209](#)

openSUSE-SU-2015:0748-1: moderate: Security update for Chromium

lists.opensuse.org
text/html

[SUSE openSUSE-SU-2015:0748](#)

Red Hat Customer Portal

web.archive.org
text/html
Inactive Link **Not Archived**

[REDHAT RHSA-2015:0816](#)

openSUSE-SU-2015:1887-1: moderate:

lists.opensuse.org

[SUSE openSUSE-SU-2015:1887](#)

Security update for chromium	text/html	
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2015/04/stable-channel-update_14.html
Issue 437399 - chromium - Heap-buffer-overflow in blink::BidiResolver::applyL1Rule - An open-source project to help move the web forward. - Google Project Hosting	code.google.com text/html	 CONFIRM code.google.com/p/chromium/issues/detail?id=437399
USN-2570-1: Oxide vulnerabilities Ubuntu	ubuntu.com text/html	 UBUNTU USN-2570-1
Chromium: Multiple vulnerabilities (GLSA 201506-04) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201506-04

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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Google	Chrome	All	All	All	All
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:a:google:chrome:*:*:*:*:*:						

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](#)