



CVE-2015-1240

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

Summary

CVE	CVE-2015-1240
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-19 10:59:00 UTC
Updated	2023-11-07 02:24:00 UTC
Description	gpu/blink/webgraphicscontext3d_impl.cc in the WebGL implementation in Google Chrome before 42.0.2311.90 allows remote attackers to execute arbitrary code via crafted WebGL programs.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	15.04	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	15.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Google	Chrome	All	All	All	All

References

Reference

Red Hat Customer Portal

Chromium: Multiple vulnerabilities (GLSA 201506-04) — Gentoo security

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

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

Issue 978193003: Fix glGetActiveUniform/Attrib crashes due to state inconsistency - Code Review

openSUSE-SU-2015:0748-1: moderate: Security update for Chromium
openSUSE-SU-2015:1887-1: moderate: Security update for chromium
Chrome Releases: Stable Channel Update
USN-2570-1: Oxide vulnerabilities Ubuntu
Issue 463599 - chromium - Heap-buffer-overflow in blink::WebString::fromUTF8 - An open-source project to help move the web forward. - Google
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 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