



CVE-2015-1221

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

Summary

CVE	CVE-2015-1221
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-09 00:59:00 UTC
Updated	2023-11-07 02:24:00 UTC
Description	Use-after-free vulnerability in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a de

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

References

Reference
Google Chrome Prior to 41.0.2272.76 Multiple Security Vulnerabilities
Chrome Releases: Stable Channel Update
Gentoo Security
Issue 455368 - chromium - UNKNOWN in blink::SQLStatementBackend::execute - An open-source project to help move the web forward. - G
[blink] Revision 190035
USN-2521-1: Oxide vulnerabilities Ubuntu
[blink] Revision 190021
Red Hat Customer Portal
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](#)