



CVE-2016-5135

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

Summary

CVE	CVE-2016-5135
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-23 19:59:00 UTC
Updated	2023-11-07 02:32:00 UTC
Description	WebKit/Source/core/html/parser/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

605451 - CSP 'referrer' directive ignored for preload requests - chromium - Monorail
[security-announce] openSUSE-SU-2016:1869-1: important: Security update
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security
[security-announce] openSUSE-SU-2016:1918-1: important: Security update
USN-3041-1: Oxide vulnerabilities Ubuntu
Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, Spoof URLs, and
Red Hat Customer Portal
[security-announce] openSUSE-SU-2016:1868-1: important: Security update
Google Chrome Prior to 52.0.2743.82 Multiple Security Vulnerabilities
[security-announce] openSUSE-SU-2016:1865-1: important: Security update
Debian -- Security Information -- DSA-3637-1 chromium-browser
Issue 1913983002: Use document referrer policy when preloading - Code Review
Chrome Releases: Stable Channel Update

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](#)