



CVE-2017-5064

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

Summary

CVE	CVE-2017-5064
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-27 05:29:00 UTC
Updated	2023-11-07 02:48:00 UTC
Description	Incorrect handling of DOM changes in Blink in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference
Issue 693974 - chromium - An open-source project to help move the web forward. - Monorail
Google Chrome Prior to 58.0.3029.81 Multiple Security Vulnerabilities
Chrome Releases: Stable Channel Update for Desktop
Google Chrome Multiple Flaws Let Remote Users Spoof URLs, Bypass Cross-Origin Restrictions, and Execute Arbitrary Code - SecurityTrack
Red Hat Customer Portal
Chromium: Multiple vulnerabilities (GLSA 201705-02) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710338](#) Gentoo Linux Chromium Multiple Vulnerabilities (GLSA 201705-02)

© [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](#)