



CVE-2016-5204

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

Summary

CVE	CVE-2016-5204
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-19 05:59:00 UTC
Updated	2023-11-07 02:33:00 UTC
Description	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for M

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Chrome Releases: Stable Channel Update for Desktop		chromereleases.googleblog.com
Chromium: Multiple vulnerabilities (GLSA 201612-11) — Gentoo Security		security.gentoo.org
Red Hat Customer Portal		rhn.redhat.com
630870 - Security: Universal XSS by intercepting a UA shadow tree - chromium - Monorail	CONFIRM	crlbug.com
Google Chrome Prior to 55.0.2883.75 Multiple Security Vulnerabilities		www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)