



CVE-2017-5077

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

Summary

CVE	CVE-2017-5077
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	Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 5

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference

Chromium: Multiple vulnerabilities (GLSA 201706-20) — Gentoo Security
716311 - Heap-buffer-overflow in SkSpecularLightingImageFilter::onFilterImage - chromium - Monorail
Chrome Releases: Stable Channel Update for Desktop
Google Chrome Multiple Flaws Let Remote Users Spoof URLs, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - Security
Google Chrome Prior to 59.0.3071.86 Multiple Security Vulnerabilities
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
710498 Gentoo Linux Chromium Multiple Vulnerabilities (GLSA 201706-20)

© [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](#)