



CVE-2018-6120

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

Summary

CVE	CVE-2018-6120
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-09 19:29:00 UTC
Updated	2023-11-07 02:59:00 UTC
Description	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to

Risk And Classification

Problem Types: CWE-787 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	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 Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-4237-1 chromium-browser	DEBIAN	www.debian.org
833721 - chromium - An open-source project to help move the web forward. - Monorail	MISC	crbug.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 201805-06) — Gentoo Security		security.gentoo.org

Google Chrome Prior to 66.0.3359.170 Multiple Security Vulnerabilities		www.securityfocus.com
Chrome Releases: Stable Channel Update for Desktop	CONFIRM	chromereleases.googleblog.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.

Legacy QID Mappings

[690612](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (e457978b-5484-11e8-9b85-54ee754af08e)

[710223](#) Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 201805-06)

© 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