



CVE-2018-6115

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-6115
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-04 17:29:00 UTC
Updated	2023-11-07 02:59:00 UTC
Description	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.117 allow

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
Application	Google	Chrome	All	All	All	All

References

Reference	Source	Link
Chrome Releases: Stable Channel Update for Desktop	CONFIRM	chromereleases.googleblog.com
Google Chrome Prior to 66.0.3359.117 Multiple Security Vulnerabilities	BID	www.securityfocus.com
819809 - chromium - An open-source project to help move the web forward. - Monorail		crbug.com
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 201804-22) — Gentoo security	GENTOO	security.gentoo.org
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

[710247](#) Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 201804-22)

© [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](#)