



CVE-2017-5084

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

Summary

CVE	CVE-2017-5084
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	Inappropriate implementation in image-burner in Google Chrome OS prior to 59.0.3071.92 allowed a local attacker to read l

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Chrome Os	All	All	All	All
Operating System	Google	Chrome Os	All	All	All	All

References

Reference	Source	Link	Tags
Chromium: Multiple vulnerabilities (GLSA 201706-20) — Gentoo Security		security.gentoo.org	
Google Chrome OS CVE-2017-5084 Local Information Disclosure Vulnerability	BID	www.securityfocus.com	Third P
Chrome Releases: Stable Channel Update for Chrome OS	MISC	chromereleases.googleblog.com	Vendo
702030 - Security: chronos user local file read (ImageBurner) - chromium - Monorail	MISC	crbug.com	Issue "
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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](#)