



CVE-2017-5073

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

Summary

CVE	CVE-2017-5073
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	Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071

Risk And Classification

Problem Types: CWE-416

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
716474 - Security: Use-after-poison in blink::FrameView::AdjustMediaTypeForPrinting - 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)