



# CVE-2017-5044

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-5044
<b>State</b>	PUBLISHED
<b>Assigner</b>	Chrome
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-24 23:59:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 5

## Risk And Classification

**Primary CVSS:** v3.1 6.3 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

**Problem Types:** CWE-787 | heap buffer overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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	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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Na	Google Chrome Prior To 57.0.2987.98 For Mac Windows And Linux And 57.0.2987.108 For Android	affected Google C

### References

Reference	Source	Link
688987 - Security: Heap Buffer OverFlow Vulnerability in Skia - chromium - Monorail	af854a3a-2127-422b-91ae-364da2661108	<a href="#">crbug.cor</a>
Google Chrome Prior to 57.0.2987.98 Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.seci</a>
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	<a href="#">rhn.redha</a>
Chromium: Multiple vulnerabilities (GLSA 201704-02) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661108	<a href="#">security.g</a>
Debian -- Security Information -- DSA-3810-1 chromium-browser	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.deb</a>
Chrome Releases: Stable Channel Update for Desktop	af854a3a-2127-422b-91ae-364da2661108	<a href="#">chromere</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710550](#) Gentoo Linux Chromium Multiple Vulnerabilities (GLSA 201704-02)

© [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](#)