CVE-2017-5044

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5044
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 23:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	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	crbug.cor
Google Chrome Prior to 57.0.2987.98 Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.sec
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redha
Chromium: Multiple vulnerabilities (GLSA 201704-02) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661108	security.g
Debian -- Security Information -- DSA-3810-1 chromium-browser	af854a3a-2127-422b-91ae-364da2661108	www.deb
Chrome Releases: Stable Channel Update for Desktop	af854a3a-2127-422b-91ae-364da2661108	chromere
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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