CVE-2017-5030

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

Summary

CVE	CVE-2017-5030
State	PUBLISHED
Assigner	Chrome
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 23:59:00 UTC
Updated	2026-04-21 17:51:06 UTC
Description	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.503140000 probability, percentile 0.978640000 (date 2026-05-14)

CISA KEV: Listed on 2022-06-08; due 2022-06-22; ransomware use Unknown

Problem Types: CWE-125 | heap buffer overflow | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
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

High

Integrity

High

Availability

High

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

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

CISA Known Exploited Vulnerability

Vendor	Google
Product	Chromium V8
Name	Google Chromium V8 Memory Corruption Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-5030

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	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

Vendor Declared Affected Products

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

References

Reference	Source	Link
Google Chrome Prior to 57.0.2987.98 Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.security
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.co
ZDI-20-126 | Zero Day Initiative	af854a3a-2127-422b-91ae-364da2661108	www.zeroday
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
Chromium: Multiple vulnerabilities (GLSA 201704-02) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661108	security.gento
682194 - Security: Out-of-bounds read in V8 Array.concat - chromium - Monorail	af854a3a-2127-422b-91ae-364da2661108	crbug.com
Debian -- Security Information -- DSA-3810-1 chromium-browser	af854a3a-2127-422b-91ae-364da2661108	www.debian.(
Chrome Releases: Stable Channel Update for Desktop	af854a3a-2127-422b-91ae-364da2661108	chromereleas
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-06-08T00:00:00.000Z	CVE-2017-5030 added to CISA KEV

Legacy QID Mappings

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