

CVE-2016-5198

Google Chromium V8 Out-of-Bounds Memory Vulnerability

CISA KEV since Jun 8, 2022

Actively exploited

V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.342 98.4th percentile · FIRST	CISA DEADLINE Jun 22, 2022 KEV since 2022 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.342 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 54.0.2840.90 < 54.0.2840.85 < 54.0.2840.87	54.0.2840.90 · 54.0.2840.85 · 54.0.2840.87	NVD
linux kernel	—	no fixed version listed	NVD
android	—	no fixed version listed	NVD
macos	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
enterprise linux desktop	6.0	no fixed version listed	NVD
enterprise linux server	6.0	no fixed version listed	NVD
enterprise linux workstation	6.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-cpfm-2p8w-wrxc

NVD nvd.nist.gov/vuln/detail/CVE-2016-5198

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2016-6149

Additional guidance chromereleases.googleblog.com/2016/11/stable-channel-update-for-desktop.html

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2016-5198

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.