

CVE-2019-5786

Google Chrome Blink Use-After-Free Vulnerability

CISA KEV since May 23, 2022

Actively exploited

Public exploit module (Metasploit)

Object lifetime issue in Blink in Google Chrome prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.611 99.16th percentile · FIRST	CISA DEADLINE Jun 13, 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	0.611 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ 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
puppeteer	< 1.13.0	1.13.0	GitHub
chrome	< 72.0.3626.121	no fixed version listed	NVD

Sources

Vendor guidance	chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html	NVD	nvd.nist.gov/vuln/detail/CVE-2019-5786
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-c2gp-86p4-5935
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-0957	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-5786

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