CVE-2020-6572

Google Chrome Media Use-After-Free Vulnerability

CISA KEV since Jan 10, 2022 | Actively exploited

Use after free in Media in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to execute arbitrary code via a crafted HTML page.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100 Urgent priority	8.8 High · NVD	0.106 95.8th percentile · FIRST	Jul 10, 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	0.106 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	< 81.0.4044.92	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-48wj-mfx4-4qc2	Additional guidance	chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_7.html
NVD	nvd.nist.gov/vuln/detail/CVE-2020-6572	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-27721	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-6572

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