CVE-2022-4262

Google Chromium V8 Type Confusion Vulnerability

CISA KEV since Dec 5, 2022 | Actively exploited

Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	8.8	0.235	Dec 26, 2022
Urgent priority	High · NVD	97.8th percentile · FIRST	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**	0.235 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	< 108.0.5359.94	no fixed version listed	NVD

Sources

Vendor guidance chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html

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

Current data evulnable.com/vulnerability-management/cve/CVE-2022-4262

NVD nvd.nist.gov/vuln/detail/CVE-2022-4262

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-51618

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