

CVE-2024-7971

Google Chromium V8 Type Confusion Vulnerability

CISA KEV since Aug 26, 2024

Actively exploited

Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.6 Critical · NVD	EPSS 0.211 97.6th percentile · FIRST	CISA DEADLINE Sep 16, 2024 KEV since 2024 · 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	0.211 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.6	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 128.0.6613.84	no fixed version listed	NVD
edge	< 128.0.2739.42	no fixed version listed	NVD

Sources

Vendor guidance	microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/	chromereleases.googleblog.com	chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
NVD	nvd.nist.gov/vuln/detail/CVE-2024-7971	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-48804	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-7971

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