

CVE-2023-4762

Google Chromium V8 Type Confusion Vulnerability

CISA KEV since Feb 6, 2024

Actively exploited

Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.414 98.7th percentile · FIRST	CISA DEADLINE Feb 27, 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	0.414 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 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	< 116.0.5845.179	no fixed version listed	NVD
edge chromium	< 116.0.1938.76	no fixed version listed	NVD
debian linux	11.0 12.0	no fixed version listed	NVD
fedora	37 38 39	no fixed version listed	NVD

Sources

Vendor guidance msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4762
NVD nvd.nist.gov/vuln/detail/CVE-2023-4762

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-54609

Additional guidance chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop.html

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

Current data evulnable.com/vulnerability-management/cve/CVE-2023-4762

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