

CVE-2026-85046

Google Chromium V8 Type Confusion Vulnerability

CISA KEV since Sep 4, 2026

Actively exploited

Type confusion in V8 in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)

EVRS 76 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.489 98.9th percentile · FIRST	CISA DEADLINE Sep 18, 2026 CISA federal deadline · Overdue by 34 days
---	--	--	---

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	Added to CISA KEV within the last 90 days
☒ EPSS	0.489 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 in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 152.0.7977.82	no fixed version listed	NVD
v8	< 15.3.48	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-84qv-4wj5-wwwm	chromereleases.googleblog.com	chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-85046	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-70702	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-85046

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