

CVE-2026-11645

Google Chromium V8 Out-of-Bounds Read and Write Vulnerability

CISA KEV since Jun 9, 2026

Actively exploited

Out of bounds read and write in V8 in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.024 84.2nd percentile · FIRST	CISA DEADLINE Jun 23, 2026 CISA federal deadline · Overdue by 4 months
---	--	--	--

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 year
☒ EPSS	0.024 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, follow applicable BOD 22-01 guidance for cloud services, 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	< 149.0.7827.103	no fixed version listed	NVD
macos	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-x2hh-w9mw-3vq2	Additional guidance	chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
issues.chromium.org	issues.chromium.org/issues/506689381	NVD	nvd.nist.gov/vuln/detail/CVE-2026-11645
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-35245
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-11645		

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