

CVE-2026-3909

Google Skia Out-of-Bounds Write Vulnerability

CISA KEV since Mar 13, 2026

Actively exploited

Out of bounds write in Skia in Google Chrome prior to 146.0.7680.75 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.023 83.5th percentile · FIRST	CISA DEADLINE Mar 27, 2026 CISA federal deadline · Overdue by 7 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	0.023 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. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 146.0.7680.80	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-vmc5-xpp6-2j82

Additional guidance chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html

NVD nvd.nist.gov/vuln/detail/CVE-2026-3909

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-11734

Current data evulnable.com/vulnerability-management/cve/CVE-2026-3909

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