

CVE-2023-7024

Google Chromium WebRTC Heap Buffer Overflow Vulnerability

CISA KEV since Jan 2, 2024

Actively exploited

Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.067 93.9th percentile · FIRST	CISA DEADLINE Jan 23, 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	0.067 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. **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	< 120.0.6099.129	no fixed version listed	NVD
debian linux	11.0 12.0	no fixed version listed	NVD
fedora	38 39	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-7c6v-f3h8-2x89	Additional guidance	chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html
NVD	nvd.nist.gov/vuln/detail/CVE-2023-7024	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-59215	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-7024

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