

CVE-2023-4863

Google Chromium WebP Heap-Based Buffer Overflow Vulnerability

CISA KEV since Sep 13, 2023

Actively exploited

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

EVRs

86/100

Immediate priority

CVSS V3.1

8.8

High · NVD

EPSS

0.999

99.98th percentile · FIRST

CISA DEADLINE

Oct 4, 2023

KEV since 2023 · 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	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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 · GHSA-j7hp-h8jx-5ppr lists 11 more affected packages · 4 more affected products on the

NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
libwebp-sys2	< 0.1.8	0.1.8	GitHub
libwebp-sys	< 0.9.3	0.9.3	GitHub
electron	≥ 22.0.0, < 22.3.24	22.3.24	GitHub
electron	≥ 24.0.0, < 24.8.3	24.8.3	GitHub
electron	≥ 25.0.0, < 25.8.1	25.8.1	GitHub
electron	≥ 26.0.0, < 26.2.1	26.2.1	GitHub
electron	≥ 27.0.0-beta.1, < 27.0.0-beta.2	27.0.0-beta.2	GitHub
SkiaSharp	≥ 2.0.0, < 2.88.6	2.88.6	GitHub
chrome	< 116.0.5845.187	no fixed version listed	NVD
firefox	< 102.15.1 < 117.0.1 ≥ 115.1.0 < 115.2.1	no fixed version listed	NVD
thunderbird	< 102.15.1 ≥ 115.0 < 115.2.2	no fixed version listed	NVD
edge chromium	< 116.0.1938.81	no fixed version listed	NVD
teams	< 1.6.00.26463 < 1.6.00.26474	no fixed version listed	NVD
webp image extension	< 1.0.62681.0	no fixed version listed	NVD
libwebp	< 1.3.2	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
active iq unified manager	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/webmproject/libwebp/commit/902bc9190331343b2017211debcec8d2ab87e17a	Additional guidance	chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
chromereleases.googleblog.com	chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html?m=1	NVD	nvd.nist.gov/vuln/detail/CVE-2023-4863
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-j7hp-h8jx-5ppr
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-2533	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-4863

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