

CVE-2023-2136

Google Chrome Skia Integer Overflow Vulnerability

CISA KEV since Apr 21, 2023

Actively exploited

Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 9.6 Critical · NVD	EPSS 0.057 93rd percentile · FIRST	CISA DEADLINE May 12, 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	0.057 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.6	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
chrome	< 112.0.5615.137	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD
fedora	36 37 38	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-63j8-q3xx-g3c2

Additional guidance chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html

NVD nvd.nist.gov/vuln/detail/CVE-2023-2136

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-33656

Current data evulnable.com/vulnerability-management/cve/CVE-2023-2136

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