

CVE-2021-30633

Google Chromium Indexed DB API Use-After-Free Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.6 Critical · NVD	EPSS 0.332 98.4th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · 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	0.332 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	< 93.0.4577.82	no fixed version listed	NVD
fedora	33 35	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-7pph-hp2f-gxfg

Additional guidance lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/4DDW7HAHTS3SDVXBQUY4SUREL05D4X7R/cisa.gov/known-exploited-vulnerabilities-catalog

NVD nvd.nist.gov/vuln/detail/CVE-2021-30633

CISA KEV

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-17553

Current data evulnable.com/vulnerability-management/cve/CVE-2021-30633

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