



CVE-2019-13720

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-13720
State	PUBLIC
Assigner	chrome-cve-admin@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-25 15:15:00 UTC
Updated	2022-10-06 03:03:00 UTC
Description	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap cc

Risk And Classification

EPSS: 0.895860000 probability, percentile 0.995560000 (date 2026-04-06)

CISA KEV: Listed on 2022-05-23; due 2022-06-13; ransomware use Unknown

Problem Types: CWE-416

CISA Known Exploited Vulnerability

Vendor	Google
Product	Chrome WebAudio
Name	Google Chrome WebAudio Use-After-Free Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-13720

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link	Ta
Google Chrome 78.0.3904.70 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
Chrome Releases: Stable Channel Update for Desktop	MISC	chromereleases.googleblog.com	Ve

[security-announce] openSUSE-SU-2019:2664-1: important: Security update	SUSE	lists.opensuse.org	
Qt WebEngine: Arbitrary code execution (GLSA 202004-04) — Gentoo security	GENTOO	security.gentoo.org	
1019226 - chromium - An open-source project to help move the web forward. - Monorail	MISC	crbug.com	Pe
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	ke



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.