



# Google Chromium V8 Out-of-Bounds Memory Access Vulnerability

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

## Summary

<b>CVE</b>	CVE-2024-0519
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-16 22:15:00 UTC
<b>Updated</b>	2024-01-22 19:53:00 UTC
<b>Description</b>	Google Chromium V8 Engine contains an out-of-bounds memory access vulnerability that allows a remote attacker to poter

## Risk And Classification

**EPSS:** 0.001420000 probability, percentile 0.342060000 (date 2026-04-01)

**CISA KEV:** Listed on 2024-01-17; due 2024-02-07; ransomware use Unknown

**Problem Types:** CWE-787

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Google
<b>Product</b>	Chromium V8
<b>Name</b>	Google Chromium V8 Out-of-Bounds Memory Access Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html">https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2024-0519">https://nvd.nist.gov/vuln/detail/CVE-2024-0519</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

## References

Reference	Source	Link
Chrome Releases: Stable Channel Update for Desktop		<a href="#">chromereleases</a>
[SECURITY] Fedora 38 Update: chromium-120.0.6099.224-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproje</a>
[SECURITY] Fedora 38 Update: chromium-120.0.6099.224-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproje</a>

[SECURITY] Fedora 39 Update: chromium-120.0.6099.224-1.fc39 - package-announce - Fedora Mailing-Lists	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
1517354 - chromium - An open-source project to help move the web forward. - Monorail	<a href="https://crbug.com/">crbug.com</a>
CVE Program record	CVE.ORG <a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD <a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA <a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">284867</a> Fedora Security Update for chromium (FEDORA-2024-049f068a8c)
<a href="#">285032</a> Fedora Security Update for chromium (FEDORA-2024-44b1f656a3)
<a href="#">379263</a> Google Chrome Prior to 120.0.6099.234 Multiple Vulnerabilities
<a href="#">379271</a> Microsoft Edge Based on Chromium Prior to 120.0.2210.144 Multiple Vulnerabilities
<a href="#">510687</a> Alpine Linux Security Update for qt6-qtwebengine
<a href="#">510689</a> Alpine Linux Security Update for qt5-qtwebengine
<a href="#">6000433</a> Debian Security Update for chromium (DSA 5602-1)
<a href="#">691399</a> Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (1bc07be0-b514-11ee-86bb-a8a1599412c6)
<a href="#">691400</a> Free Berkeley Software Distribution (FreeBSD) Security Update for electron26 (2264566a-a890-46eb-a895-7881dd220bd0)
<a href="#">691406</a> Free Berkeley Software Distribution (FreeBSD) Security Update for qt6 (a25b323a-bed9-11ee-bdd6-4ccc6adda413)
<a href="#">691407</a> Free Berkeley Software Distribution (FreeBSD) Security Update for qt5 (a11e7dd1-bed4-11ee-bdd6-4ccc6adda413)
<a href="#">710863</a> Gentoo Linux QtWebEngine Multiple Vulnerabilities (GLSA 202402-14)
<a href="#">710872</a> Gentoo Linux Chromium, Google Chrome, Microsoft Edge Multiple Vulnerabilities (GLSA 202402-23)
<a href="#">755652</a> OpenSUSE Security Update for opera (openSUSE-SU-2024:0033-1)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)