



# CVE-2023-2724

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

## Summary

<b>CVE</b>	CVE-2023-2724
<b>State</b>	PUBLIC
<b>Assigner</b>	chrome-cve-admin@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-16 19:15:00 UTC
<b>Updated</b>	2023-11-25 11:15:00 UTC
<b>Description</b>	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corrup

## Risk And Classification

### Problem Types: CWE-843

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All

## References

Reference	Source	Link
Chromium, Google Chrome, Microsoft Edge: Multiple Vulnerabilities (GLSA 202309-17) — Gentoo security	MISC	<a href="#">security.gentoo.</a>
Chrome Internal JavaScript Object Access Via Origin Trials ≈ Packet Storm	MISC	<a href="#">packetstormseci</a>
Debian -- Security Information -- DSA-5404-1 chromium	MISC	<a href="#">www.debian.org</a>
QtWebEngine: Multiple Vulnerabilities (GLSA 202311-11) — Gentoo security		<a href="#">security.gentoo.</a>
Chrome Releases: Stable Channel Update for Desktop	MISC	<a href="#">chromereleases</a>
[SECURITY] Fedora 37 Update: chromium-113.0.5672.126-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproje</a>
1433211 - chromium - An open-source project to help move the web forward. - Monorail	MISC	<a href="#">crbug.com</a>
[SECURITY] Fedora 38 Update: chromium-113.0.5672.126-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproje</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

181790	Debian Security Update for chromium (DSA 5404-1)
182555	Debian Security Update for chromium (CVE-2023-2724)
283992	Fedora Security Update for chromium (FEDORA-2023-69264c19f9)
284109	Fedora Security Update for chromium (FEDORA-2023-5c477a04ca)
378496	Google Chrome Prior to 113.0.5672.126 Multiple Vulnerabilities
378502	Microsoft Edge Based on Chromium Prior to 113.0.1774.50 Multiple Vulnerabilities
691170	Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (bea52545-f4a7-11ed-8290-a8a1599412c6)
691192	Free Berkeley Software Distribution (FreeBSD) Security Update for electron22 (3c3d3dcb-bef7-4d20-9580-b4216b5ff6a2)
691193	Free Berkeley Software Distribution (FreeBSD) Security Update for electron23 (3bf6795c-d44c-4033-9b37-ed2e30f34fca)
710759	Gentoo Linux Chromium, Google Chrome, Microsoft Edge Multiple Vulnerabilities (GLSA 202309-17)
710797	Gentoo Linux QtWebEngine Multiple Vulnerabilities (GLSA 202311-11)
754045	OpenSUSE Security Update for opera (openSUSE-SU-2023:0114-1)
754103	OpenSUSE Security Update for opera (openSUSE-SU-2023:0115-1)

© 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**