



# CVE-2026-7950

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

## Summary

<b>CVE</b>	CVE-2026-7950
<b>State</b>	PUBLISHED
<b>Assigner</b>	Chrome
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 19:16:43 UTC
<b>Updated</b>	2026-05-07 02:09:44 UTC
<b>Description</b>	Out of bounds read and write in GFX in Google Chrome prior to 148.0.7778.96 allowed a remote attacker to perform arbitra

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from ADP

**CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N**

**Problem Types:** CWE-125 | CWE-787 | Out of bounds read and write | CWE-125 CWE-125 Out-of-bounds Read | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.4	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N</b>
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.4	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**Required**

Scope

**Unchanged**

Confidentiality

**Low**

Integrity

**Low**

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Google</a>	<a href="#">Chrome</a>	affected 148.0.7778.96 148.0.7778.96 custom	Not specified

### References

Reference	Source	Link
<a href="https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html">chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html</a>	<a href="mailto:chrome-cve-admin@google.com">chrome-cve-admin@google.com</a>	<a href="https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html">chromereleases.googleblog.com</a>
<a href="https://issues.chromium.org/issues/496259890">issues.chromium.org/issues/496259890</a>	<a href="mailto:chrome-cve-admin@google.com">chrome-cve-admin@google.com</a>	<a href="https://issues.chromium.org/issues/496259890">issues.chromium.org</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>

No vendor comments have been submitted for this CVE.

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

© 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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

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