



# Memory safety bugs fixed in Firefox 149 and Thunderbird 149

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

## Summary

<b>CVE</b>	CVE-2026-4729
<b>State</b>	PUBLISHED
<b>Assigner</b>	mozilla
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-24 13:16:08 UTC
<b>Updated</b>	2026-04-13 15:17:45 UTC
<b>Description</b>	Memory safety bugs present in Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corrupt

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from ADP

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

**EPSS:** 0.000200000 probability, percentile 0.052830000 (date 2026-04-15)

**Problem Types:** CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	unaffected 149 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 149 * rpm	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.mozilla.org/security/advisories/mfsa2026-23">www.mozilla.org/security/advisories/mfsa2026-23</a>	security@mozilla.org	<a href="http://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
<a href="http://www.mozilla.org/security/advisories/mfsa2026-20">www.mozilla.org/security/advisories/mfsa2026-20</a>	security@mozilla.org	<a href="http://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
<a href="http://bugzilla.mozilla.org/buglist.cgi">bugzilla.mozilla.org/buglist.cgi</a>	security@mozilla.org	<a href="http://bugzilla.mozilla.org">bugzilla.mozilla.org</a>	Broken Link
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Christian Holler, Fatih Kilic, Tom Schuster and the Mozilla Fuzzing Team (en)

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

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)