



# Use-after-free in the Widget: Cocoa component

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-6759  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | mozilla  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-04-21 13:16:21 UTC  |
| <b>Updated</b>         | 2026-04-22 16:08:03 UTC  |
| <b>Description</b>     | Use-after-free in the Widget: Cocoa component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbir |

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

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

**EPSS:** 0.000440000 probability, percentile 0.136450000 (date 2026-04-22)

**Problem Types:** CWE-416 | CWE-416 CWE-416 Use After Free

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1     | ADP                                  | DECLARED  | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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 | 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 140.10 140.* rpm | Not specified |
| CNA    | Mozilla | Firefox     | unaffected 150 * rpm        | Not specified |
| CNA    | Mozilla | Thunderbird | unaffected 140.10 140.* rpm | Not specified |
| CNA    | Mozilla | Thunderbird | unaffected 150 * rpm        | Not specified |

### References

| Reference                                       | Source               | Link                 | Tags                 |
|---|----------------------|----------------------|----------------------|
| bugzilla.mozilla.org/show_bug.cgi               | security@mozilla.org | bugzilla.mozilla.org | Permissions Required |
| www.mozilla.org/security/advisories/mfsa2026-34 | security@mozilla.org | www.mozilla.org      | Vendor Advisory      |
| www.mozilla.org/security/advisories/mfsa2026-30 | security@mozilla.org | www.mozilla.org      | Vendor Advisory      |
| www.mozilla.org/security/advisories/mfsa2026-32 | security@mozilla.org | www.mozilla.org      | Vendor Advisory      |
| www.mozilla.org/security/advisories/mfsa2026-33 | security@mozilla.org | www.mozilla.org      | Vendor Advisory      |
| CVE Program record                              | CVE.ORG              | www.cve.org          | canonical            |
| NVD vulnerability detail                        | NVD                  | nvd.nist.gov         | canonical, analysis  |

### Vendor Comments And Credit

Discovery Credit

**CNA:** Steven Michaud (en)

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

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)