



Sandboxed iframes allowed links to open in external apps (Android only)

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-11716 |
| State | PUBLISHED |
| Assigner | mozilla |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-10-14 13:15:37 UTC |
| Updated | 2026-04-13 15:16:40 UTC |
| Description | Links in a sandboxed iframe could open an external app on Android without the required "allow-" permission. This vulnerabi |

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.000280000 probability, percentile 0.079560000 (date 2026-04-15)

Problem Types: CWE-284 | CWE-284 CWE-284 Improper Access Control

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | ADP | DECLARED | 6.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 6.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------|-------------|---------|--------|---------|----------|
| Operating System | Google | Android | - | 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 144 * rpm | Not specified |
| CNA | Mozilla | Thunderbird | unaffected 144 * rpm | Not specified |

References

| Reference | Source | Link | Tags |
|---|----------------------|----------------------|--------------------------------------|
| bugzilla.mozilla.org/show_bug.cgi | security@mozilla.org | bugzilla.mozilla.org | Issue Tracking, Permissions Required |
| www.mozilla.org/security/advisories/mfsa2025-84 | security@mozilla.org | www.mozilla.org | Vendor Advisory |
| www.mozilla.org/security/advisories/mfsa2025-81 | 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: Axel Chong (@Haxatron) (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](#) 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

CVE.report and Source URL Uptime Status status.cve.report