Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4689
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 13:16:04 UTC
Updated	2026-04-13 15:17:37 UTC
Description	Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability was fi

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from nvd@nist.gov

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

Problem Types: CWE-190 | CWE-754 | CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	ADP	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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	Firefox	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mozilla	Firefox	unaffected 115.34 115.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 140.9 140.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 149 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 140.9 140.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 149 * rpm	Not specified

References

Reference	Source	Link	Tags
www.mozilla.org/security/advisories/mfsa2026-24	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-23	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-22	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-21	security@mozilla.org	www.mozilla.org	Vendor Advisory
www.mozilla.org/security/advisories/mfsa2026-20	security@mozilla.org	www.mozilla.org	Vendor Advisory
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Permissions Required
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: Sajeeb Lohani (en)

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

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

Free CVE JSON API cve.report/api

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