JavaScript engine only wrote partial return value to stack

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

Summary

CVE	CVE-2025-8027
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-22 21:15:49 UTC
Updated	2026-04-13 15:17:08 UTC
Description	On 64-bit platforms IonMonkey-JIT only wrote 32 bits of the 64-bit return value space on the stack. Baseline-JIT, however, r

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:H/I:N/A:N

Problem Types: CWE-457 | CWE-457 CWE-457 Use of Uninitialized Variable

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:H/I:N/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:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

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 115.26 115.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 128.13 128.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 140.1 140.* rpm	Not specified
CNA	Mozilla	Firefox	unaffected 141 * rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 128.13 128.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 140.1 140.* rpm	Not specified
CNA	Mozilla	Thunderbird	unaffected 141 * rpm	Not specified

References

Reference	Source	Link	Tags
www.mozilla.org/security/advisories/mfsa2025-59	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-58	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-56	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-57	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-62	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-63	security@mozilla.org	www.mozilla.org	Vendor Ad
www.mozilla.org/security/advisories/mfsa2025-61	security@mozilla.org	www.mozilla.org	Vendor Ad
bugzilla.mozilla.org/show_bug.cgi	security@mozilla.org	bugzilla.mozilla.org	Permissior
lists.debian.org/debian-lts-announce/2025/07/msg00016.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Nan Wang (en)

CNA: Nan Wang (en)

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

Free CVE JSON API cve.report/api

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