

CVE-2019-17026

Mozilla Firefox And Thunderbird Type Confusion Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 68.4.1, Thunderbird < 68.4.1, and Firefox < 72.0.1.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.463 98.8th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.463 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
firefox	< 68.4.1 < 72.0.1	no fixed version listed	NVD
thunderbird	< 68.4.1	no fixed version listed	NVD
ubuntu linux	16.04	no fixed version listed	NVD

Sources

Vendor guidance	mozilla.org/security/advisories/mfsa2020-03/	NVD	nvd.nist.gov/vuln/detail/CVE-2019-17026
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-7500
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-17026		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.