

CVE-2024-9680

Mozilla Firefox Use-After-Free Vulnerability

Exigent

CISA KEV since Oct 15, 2024

Actively exploited

Ransomware use known

An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines. We have had reports of this vulnerability being exploited in the wild. This vulnerability affects Firefox < 131.0.2, Firefox ESR < 128.3.1, Firefox ESR < 115.16.1, Thunderbird < 131.0.1, Thunderbird < 128.3.1, and Thunderbird < 115.16.0.

EVRS 85 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.232 97.8th percentile · FIRST	CISA DEADLINE Nov 5, 2024 KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.232 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
firefox	< 115.16.1 < 131.0.2 ≥ 128.1.0 < 128.3.1	no fixed version listed	NVD
thunderbird	< 115.16.0 ≥ 128.0.1 < 128.3.1 131.0	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD

Sources

Vendor guidance msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49039**NVD** nvd.nist.gov/vuln/detail/CVE-2024-9680**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2024-50087**mozilla.org** mozilla.org/en-US/security/advisories/mfsa2024-51/**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2024-9680

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