

CVE-2016-9079

Mozilla Firefox, Firefox ESR, and Thunderbird Use-After-Free Vulnerability

CISA KEV since Jun 22, 2023

Actively exploited

Public exploit module (Metasploit)

A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.

EVRS 81/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.874 99.76th percentile · FIRST	CISA DEADLINE Jul 13, 2023 KEV since 2023 · 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	0.874 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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 · 3 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
thunderbird	< 45.5.1	no fixed version listed	NVD
firefox	< 50.0.2 < 45.5.1	no fixed version listed	NVD
tor	—	no fixed version listed	NVD
debian linux	9.0	no fixed version listed	NVD
enterprise linux	5.0 6.0 7.0	no fixed version listed	NVD
enterprise linux desktop	5.0 6.0 7.0	no fixed version listed	NVD
enterprise linux server	5.0 6.0 7.0	no fixed version listed	NVD
enterprise linux server aus	7.3 7.4	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-cmgc-v5fc-wx68	Additional guidance	bugzilla.mozilla.org/show_bug.cgi?id=1321066
mozilla.org	mozilla.org/en-US/security/advisories/mfsa2016-92/#CVE-2016-9079	NVD	nvd.nist.gov/vuln/detail/CVE-2016-9079
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-9900
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-9079		

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