

CVE-2015-4495

Mozilla Firefox Security Feature Bypass Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Public exploit module (Metasploit)

The PDF reader in Mozilla Firefox before 39.0.3, Firefox ESR 38.x before 38.1.1, and Firefox OS before 2.2 allows remote attackers to bypass the Same Origin Policy, and read arbitrary files or gain privileges, via vectors involving crafted JavaScript code and a native setter, as exploited in the wild in August 2015.

EVRS 77 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.686 99.34th percentile · FIRST	CISA DEADLINE Jun 15, 2022 KEV since 2022 · 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	0.686 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 · 7 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
firefox	< 39.0.3 ≥ 38.0 < 38.1.1	no fixed version listed	NVD
linux enterprise debuginfo	11	no fixed version listed	NVD
firefox os	< 2.2	no fixed version listed	NVD
solaris	11.3	no fixed version listed	NVD
ubuntu linux	12.04 14.04 15.04	no fixed version listed	NVD
enterprise linux desktop	5.0 6.0 7.0	no fixed version listed	NVD
enterprise linux eus	6.7 7.1 7.2 7.3 7.4 7.5 7.6 7.7	no fixed version listed	NVD
enterprise linux server	5.0 6.0 7.0	no fixed version listed	NVD

Sources

Vendor guidance	blog.mozilla.org/security/2015/08/06/firefox-exploit-found-in-the-wild/	NVD	nvd.nist.gov/vuln/detail/CVE-2015-4495
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-4515
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-4495		

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