

CVE-2018-11776

Apache Struts Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when alwaysSelectFullNamespace is true (either by user or a plugin like Convention Plugin) and then: results are used with no namespace and in same time, its upper package have no or wildcard namespace and similar to results, same possibility when using url tag which doesn't have value and action set and in same time, its upper package have no or wildcard namespace.

EVRS 85/100 Immediate priority	CVSS V3.1 8.1 High · NVD	EPSS 0.999 99.99th 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	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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
org.apache.struts:struts2-core	≥ 2.0.4, ≤ 2.3.34	2.3.35	GitHub
org.apache.struts:struts2-core	≥ 2.5, ≤ 2.5.16	2.5.17	GitHub
struts	≥ 2.0.4 < 2.3.35 ≥ 2.5.0 < 2.5.17	2.3.35 · 2.5.17	NVD
active iq unified manager	≥ 7.3 ≥ 9.5	no fixed version listed	NVD
oncommand insight	—	no fixed version listed	NVD
oncommand workflow automation	—	no fixed version listed	NVD
snapcenter	—	no fixed version listed	NVD
communications policy management	< 12.5.0	12.5.0	NVD
enterprise manager base platform	13.3.0.0 13.4.0.0	no fixed version listed	NVD
mysql enterprise monitor	≤ 3.4.9.4237 ≥ 4.0.0 ≤ 4.0.6.5281 ≥ 8.0.0 ≤ 8.0.2.8191	after 3.4.9.4237 · after 4.0.6.5281 · after 8.0.2.8191	NVD

Sources

Vendor guidance	oracle.com/technetwork/security-advisory/cpujan2019-5072801.html	NVD	nvd.nist.gov/vuln/detail/CVE-2018-11776
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-cr6j-3jp9-rw65
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2018-0582	Current data	evulnable.com/vulnerability-management/cve/CVE-2018-11776

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