

CVE-2017-9805

Apache Struts Deserialization of Untrusted Data Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

The REST Plugin in Apache Struts 2.1.1 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for deserialization without any type filtering, which can lead to Remote Code Execution when deserializing XML payloads.

EVRs

85/100

Immediate priority

CVSS V3.1

8.1

High · NVD

EPSS

0.994

99.94th 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	0.994 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-rest-plugin	≥ 2.5.0, < 2.5.13	2.5.13	GitHub
org.apache.struts:struts2-rest-plugin	≥ 2.1.1, < 2.3.34	2.3.34	GitHub
struts	≥ 2.1.2 < 2.3.34 ≥ 2.5.0 < 2.5.13	2.3.34 · 2.5.13	NVD
digital media manager	—	no fixed version listed	NVD
hosted collaboration solution	10.5\ (1\ 11.0\ (1\ 11.5\ (1\ 11.6\ (1\	no fixed version listed	NVD
media experience engine	3.5 3.5.2	no fixed version listed	NVD
network performance analysis	—	no fixed version listed	NVD
video distribution suite for internet streaming	—	no fixed version listed	NVD
oncommand balance	—	no fixed version listed	NVD



Sources

Vendor guidance blogs.apache.org/foundation/entry/apache-struts-statement-on-euifax

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-0602

NVD nvd.nist.gov/vuln/detail/CVE-2017-9805

GitHub advisory github.com/advisories/GHSA-gg9m-fj3v-r58c

Current data evulnable.com/vulnerability-management/cve/CVE-2017-9805

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