

CVE-2016-4437

Apache Shiro Code Execution Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Apache Shiro before 1.2.5, when a cipher key has not been configured for the "remember me" feature, allows remote attackers to execute arbitrary code or bypass intended access restrictions via an unspecified request parameter.

EVRS

85/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.930

99.83rd 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	0.930 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.shiro:shiro-core	≤ 1.2.4	1.2.5	GitHub
aurora	≥ 0.10.0 < 0.18.1	no fixed version listed	NVD
shiro	< 1.2.5	no fixed version listed	NVD
fuse	1.0	no fixed version listed	NVD
jboss middleware text-only advisories	1.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p836-389h-j692	NVD	nvd.nist.gov/vuln/detail/CVE-2016-4437
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-4711
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-4437		

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