CVE-2021-35464

ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability

Exigent | CISA KEV since Nov 3, 2021 | Actively exploited | Ransomware use known | Public exploit module (Metasploit)

ForgeRock AM server before 7.0 has a Java deserialization vulnerability in the jato.pageSession parameter on multiple pages. The exploitation does not require authentication, and remote code execution can be triggered by sending a single crafted /ccversion/* request to the server. The vulnerability exists due to the usage of Sun ONE Application Framework (JATO) found in versions of Java 8 or earlier

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
94/100 Immediate priority	9.8 Critical · NVD	0.999 99.99th percentile · FIRST	Nov 17, 2021 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	Known ransomware campaigns	− KEV recency	On the CISA KEV catalog for over two years
✓ EPSS	0.999 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
access management	< 6.5.4	6.5.4	NVD
openam	⩾ 9.0.0 < 14.6.3	14.6.3	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-6x75-vwp5-q242	Additional guidance	backstage.forgerock.com/knowledge/kb/article/a47894244
NVD	nvd.nist.gov/vuln/detail/CVE-2021-35464	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-22106	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-35464

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