CVE-2021-35464

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-35464
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-22 18:15:00 UTC
Updated	2021-08-02 18:03:00 UTC
Description	ForgeRock AM server before 7.0 has a Java deserialization vulnerability in the jato.pageSession parameter on multiple pag

Risk And Classification

EPSS: 0.943860000 probability, percentile 0.999710000 (date 2026-04-02)

CISA KEV: Listed on 2021-11-03; due 2021-11-17; ransomware use Known

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	ForgeRock
Product	Access Management (AM)
Name	ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-35464

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Forgerock	Am	All	All	All	All
Application	Forgerock	Openam	All	All	All	All

References

Reference	Source	Link	Tags
ForgeRock / OpenAM Jato Java Deserialization ≈ Packet Storm	MISC	packetstormsecurity.com	
System Dashboard - ForgeRock JIRA	MISC	bugster.forgerock.org	
ForgeRock Access Manager/OpenAM 14.6.3 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	

AM Security Advisory #202104 - Knowledge - BackStage	CONFIRM	backstage.forgerock.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150623 ForgeRock Access Management Remote Code Execution Vulnerability (CVE-2021-35464)

730675 ForgeRock Access Management and OpenAM Remote Code Execution (RCE) Vulnerability