Threat Brief

Updated Sep 2, 2026 - 12:27 AM EDT - askanything-app.com

ACTIVELY EXPLOITED

JFrog Artifactory auth-bypass exploited within days of disclosure - attackers minting admin tokens

WHAT HAPPENED

A critical authentication-bypass flaw in JFrog Access (which issues Artifactory credentials) lets an unauthenticated attacker forge a "phantom" join key and mint admin-level tokens; watchTowr confirmed in-the-wild exploitation used to enumerate users, groups, credentials, and federated access topologies just days after the patch landed.

AFFECTED

Artifactory 7.111.4-7.111.21, 7.117.0-7.117.27, 7.125.0-7.125.19, 7.133.0-7.133.28, 7.146.0-7.146.36, and 7.161.0-7.161.19 (self-hosted instances without an additional join key configured).

EXPLOITATION

actively exploited in the wild (watchTowr, reported via The Hacker News).

FIX

upgrade to 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, or 7.161.20.

CHECK IF YOU'RE EXPOSED

confirm an additional join key is configured; after patching, audit for unexpected admin tokens, review access logs for anomalous token-minting or enumeration of users/groups/credential sets, and rotate all credentials on internet-exposed instances.

SOURCE

[The Hacker News - Attackers Exploit Critical JFrog Artifactory Flaw to Mint Admin Tokens](https://thehackernews.com/2026/09/attackers-exploit- critical-jfrog.html) - Sep 1, 2026

Aurora ransomware affiliate caught using AI coding agent Cursor to plan intrusions - email-bombing/vishing was the way in

WHAT HAPPENED

An exposed open directory belonging to a Russian-speaking Aurora ransomware affiliate revealed months of operational logs showing the actor using the Cursor AI coding assistant (running on Claude Sonnet) as an active planning tool during real intrusions against 20+ organizations across nine countries, with initial access via email-bombing followed by IT-helpdesk vishing calls.

AFFECTED

No specific product vulnerability - this is a TTP/tooling exposure covering organizations targeted between April and July 2026, explicitly excluding CIS-region targets.

EXPLOITATION

not a CVE - actively used in real-world ransomware operations (CloudSEK and Gambit Security research, reported via The Hacker News).

FIX

N/A (process/tooling issue) - harden helpdesk identity-verification procedures and add controls against email-bombing-triggered support calls.

CHECK IF YOU'RE EXPOSED

watch for the Windows encryptor sap.exe, Linux/ESXi encryptor encrypt.out, and the ESXi/vCenter discovery script esxi_finder.py; flag help-desk call volume spikes immediately following inbound email floods, and monitor for anomalous

SMB/LDAP/WinRM/RDP/RPC lateral movement after a helpdesk-impersonation call.

SOURCE

[The Hacker News - Aurora Ransomware Operators Use Cursor AI in Attacks Against 10 Targets](https://thehackernews.com/2026/08/aurora-ransomware -operators-use-cursor.html) - Aug 31, 2026