GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 303: JFrog Artifactory Anonymous-Token Authentication Bypass Chained with Privilege Escalation - Actively Exploited (CVE-2026-42018).

Release Date: 11th September 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate a self-hosted JFrog Artifactory instance. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-42018 is a high-severity authentication flaw in JFrog Artifactory, a widely-used enterprise binary/artifact repository manager (CERTVU has previously judged JFrog Artifactory relevant to Vanuatu - see Advisory 240, CVE-2026-82329).

What are the systems affected?

The following version(s) are affected:

- JFrog Artifactory prior to 7.111.20, and 7.117.0–7.117.26, 7.125.0–7.125.18, 7.133.0–7.133.27, and 7.146.0–7.146.7 - (Affected)

JFrog Artifactory 7.111.20, 7.117.27, 7.125.19, 7.133.28, 7.146.8, and later on each respective branch - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Obtain an internal anonymous-user token without authenticating**
    - A remote, unauthenticated attacker sends a crafted HTTP request (observed as a POST to "/access/api/v1/aws/token/" with a trailing slash) to a reachable Artifactory instance, which improperly returns a valid internal anonymous-user access token even though anonymous access is disabled.
2. **Escalate the anonymous token to administrator scope and plant a backdoor**
    - Where the instance is also vulnerable to the companion privilege-escalation flaw, CVE-2026-42016, the attacker exchanges the low-privileged anonymous token for one with administrator scope, creates new administrator accounts, and installs persistent backdoors.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade JFrog Artifactory to the fixed version for your release branch (7.111.20, 7.117.27, 7.125.19, 7.133.28, or 7.146.8, or later), and separately confirm you are also running 7.133.11 or later to close the CVE-2026-42016 escalation path this flaw is actively chained with.

2. Restrict network access to the Artifactory instance where patching must be delayed
3. Audit for signs of prior compromise before and after patching
4. Rotate credentials and hunt for planted backdoors

Report any suspected compromise of a JFrog Artifactory instance to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-42018
2. https://www.wiz.io/blog/artifactory-under-attack-in-the-wild-exploitation-of-cve-2026-42016-cve-2026-4201