

**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

11th September 2026

**Advisory 304: JFrog Artifactory Token Scope Validation Flaw Leading to
Privilege Escalation - Actively Chained for Admin Takeover (CVE-2026-42016).**

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-2026-42016 is a high-severity privilege escalation vulnerability 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, and Advisory 303, CVE-2026-42018). Artifactory versions before 7.133.11 validate a presented token's signature and issuer, but fail to validate its authorized scope - allowing a holder of any valid, low-privileged token to present it to a privileged API endpoint and have it treated as administrator-scoped.

What are the systems affected?

The following version(s) are affected:

- JFrog Artifactory (Self Hosted), all versions prior to 7.133.11 - (Affected)

JFrog Artifactory 7.133.11 and later - (Not affected, patched); the fix has also been backported to earlier release branches as 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, and 7.161.20

What does this mean?

Typical attack flow:

1. **Hold or obtain any valid, low-privileged Artifactory access token**
 - An attacker holding any valid Artifactory access token - including one improperly obtained via a separate flaw such as CVE-2026-42018's anonymous-token exposure - presents it to a privileged API endpoint.
2. **Have the token treated as administrator-scoped and take over the instance**
 - Because Artifactory validates only the token's signature and issuer and not its authorized scope, the low-privileged token is accepted as if it carried administrator scope, letting the attacker create new administrator accounts and install persistent backdoors on the instance.

Successful exploitation may allow attackers to:

- Escalate a low-privileged Artifactory access token to full administrator scope, without the token itself needing to be validly issued at that privilege level.
- Gain full administrative control of the Artifactory instance, create rogue admin accounts, and install persistent backdoors across the software supply chain the repository serves.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately
 - Upgrade JFrog Artifactory to 7.133.11 or later, or the corresponding backported fix for your release branch (7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, or 7.161.20), and confirm you have also applied the fix for CVE-2026-42018 (Advisory 303), since the two are actively chained together in the wild.
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-2026-42016>
2. <https://github.com/advisories/GHSA-58cv-8cfm-c8r8>