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

3 September 2026

Advisory 240: JFrog Artifactory Authentication Bypass Leading to Administrator Takeover (CVE-2026-82329).

Release Date: 2nd September 2026
Impact: CRITICAL
TLP: CLEAR

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

This alert is relevant to Organizations, System/Network administrators, and DevOps/CI-CD engineering teams that deploy or operate JFrog Artifactory as a self-hosted binary and artifact repository manager. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-82329 is a critical authentication-bypass vulnerability leading to full administrator takeover in JFrog Artifactory, a widely-deployed binary and artifact repository manager used to centralize packages, containers, AI models, and CI/CD credentials across software development and distribution pipelines. The flaw sits in JFrog Access, Artifactory's credential-issuing and validation component: under default configuration, an Artifactory instance that has not had an additional "join key" explicitly configured is issued a predictable "phantom" default join key. An unauthenticated attacker with network access to the instance can abuse this phantom join key to forge valid-looking access tokens and mint administrator-level credentials for themselves, without ever presenting a real, previously-issued credential.

What are the systems affected?

The following version(s) are affected:

- JFrog Artifactory before 7.111.21, and each of the 7.117.x, 7.125.x, 7.133.x, 7.146.x, and 7.161.x branches prior to their respective fixes below – (Affected)

JFrog Artifactory 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, 7.161.20, and later on each respective branch – (Not affected, patched)

JFrog reports that its own SaaS/cloud-hosted Artifactory environments have already been patched automatically; this does not apply to self-hosted (on-premises or self-managed cloud) deployments, which require a deliberate upgrade. Organizations should confirm the running version directly via the Artifactory admin console rather than assuming a cloud-style automatic update has applied, and should specifically confirm whether an additional join key has been configured, since instances relying on the default phantom join key are the ones directly exploitable.

What does this mean?

Typical attack flow:

1. **Forge a valid access token using the default phantom join key**
    - An attacker with network access to a reachable Artifactory instance that has not had a custom join key configured abuses the predictable default "phantom" join key issued by JFrog Access to forge a token that Artifactory accepts as legitimate, without ever presenting a real, previously-issued credential.
2. **Mint administrator credentials and take over the instance**
    - Using the forged token, the attacker mints themselves a full administrator-level credential, then uses it to enumerate users, groups, credential sets, and any federated access topologies connected to the instance, and to create backdoor user accounts for persistent access.

Attack vectors:

- A network-based, unauthenticated request against any internet- or network-reachable Artifactory instance running an affected version with no custom join key configured.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N) — active exploitation observed in the wild confirms this is readily achievable in practice, not just in theory.

Successful exploitation may allow attackers to:

- Gain full administrative control over the Artifactory instance, including all repositories, artifacts, packages, containers, and AI models it stores or serves to downstream build and deployment pipelines.
- Create backdoor user accounts for persistent access, harvest CI/CD and federated credentials stored in or accessible through the instance, and tamper with stored artifacts — potentially poisoning the software supply chain for every downstream system that consumes packages from the compromised instance.

Indicators of Compromise:

Given confirmed active exploitation, organizations running an affected, internet- or network-reachable Artifactory instance should review for the following:

- Administrator tokens or access tokens created without a corresponding, legitimate authenticated administrator session in Artifactory's own access/audit logs.
- Unexpected or unrecognized user or group accounts, particularly ones with administrative privileges that cannot be attributed to a known administrator action.
- Unusual API enumeration activity against users, groups, credential, or federated-access-topology endpoints, and web server / reverse-proxy access logs showing unauthenticated requests to JFrog Access token-issuing endpoints from unexpected or unfamiliar source IP addresses.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade self-hosted Artifactory instances to the fixed version for your release branch (7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, or 7.161.20, per JFrog's own Security Advisories page). Cloud/SaaS Artifactory environments have already been patched by JFrog automatically, but this should still be confirmed rather than assumed.

2. Configure a custom join key on every self-hosted instance immediately, even before patching, since the default phantom join key is the specific weakness attackers are exploiting
3. Audit the estate for Artifactory deployments
4. Treat any internet-reachable, unpatched instance as potentially compromised
5. Rotate credentials and review downstream systems

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-82329
2. https://docs.jfrog.com/releases/docs/jfrog-security-advisories