Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

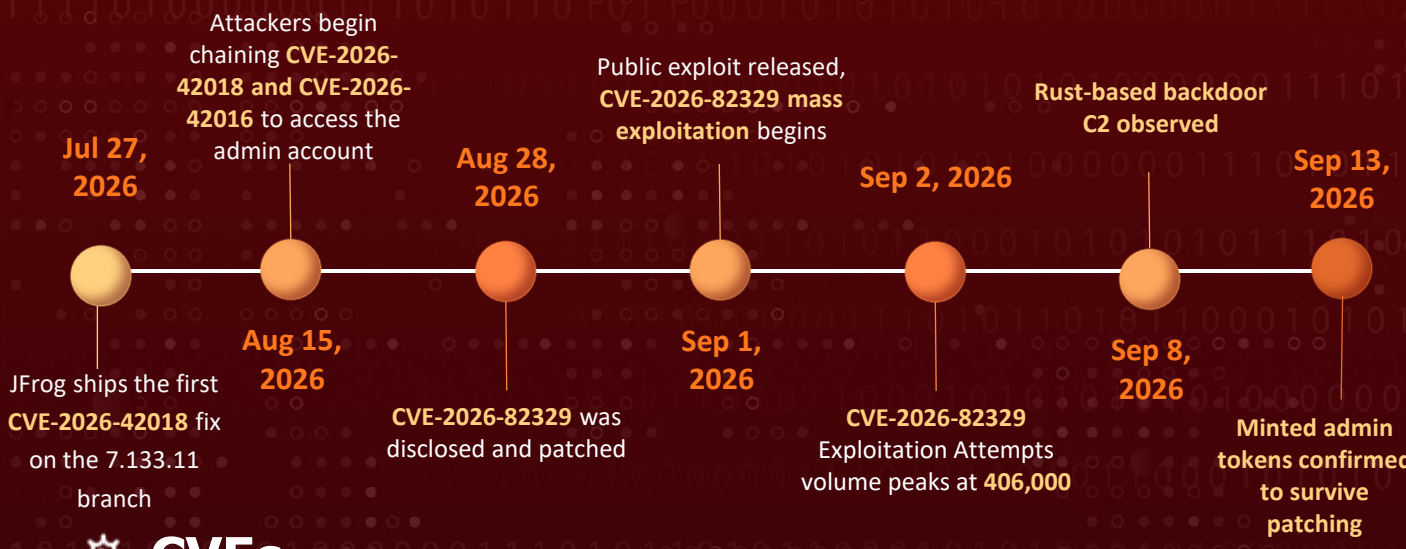
JFrog Artifactory Flaws Chained for Administrative Takeover

Date of Publication	Admiralty Code	TA Number
September 18, 2026	A1	TA2026275

Summary

First Seen: August 15, 2026
Malware: Unnamed custom Rust-based backdoor and uploaded webshells
Affected Products: JFrog Artifactory Self-Hosted (Self-Managed)
Impact: Attackers have exploited three JFrog Artifactory Self-Hosted flaws in the wild to gain full administrative control of internet-reachable repositories. CVE-2026-42018 leaks an internal anonymous-user JWT to unauthenticated callers, CVE-2026-42016 lets that token be swapped for administrator scope, and the two chained together produce a persistent admin account. Exploitation ran from August 15 to September 8, 2026, peaking near 406,000 attempts in a single day, with attackers creating rogue admin accounts, stealing configuration and join keys, installing malicious Groovy plugins, and deploying a Rust backdoor. Critically, patching does not revoke tokens already minted, so upgrading alone leaves compromised instances compromised.

Timeline



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-42016	JFrog Artifactory Incorrect Authorization Vulnerability	JFrog Artifactory Self-Hosted	✗	✓	✓
CVE-2026-42018	JFrog Artifactory Improper Authentication Vulnerability	JFrog Artifactory Self-Hosted	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-82329	JFrog Artifactory Improper Authentication Vulnerability	JFrog Artifactory Self-Hosted	✗	✓	✓

Vulnerability Details

#1

Three vulnerabilities in JFrog Artifactory Self-Hosted have been exploited in the wild to seize complete administrative control of internet-reachable artifact repositories. CVE-2026-42018 causes Artifactory to return an internal anonymous-user JSON Web Token to a caller who has never authenticated, and it does so even when anonymous access has been explicitly disabled. CVE-2026-42016 then allows that low-privilege token to be exchanged for one carrying administrator scope, because Artifactory validates a token's signature and issuer without properly enforcing its intended scope. Chained together, these two flaws move an unauthenticated attacker to a persistent administrator account.

#2

CVE-2026-82329 is a separate and more severe defect in the JFrog Access service that requires no chaining at all. On default installations, the trusted cluster join key list is built by splitting a configuration string on commas without filtering empty entries, so an empty string is registered as a live join key with a deterministic signing secret. An attacker can forge an HS256 JWT whose key identifier is the SHA-256 hash of the empty string, present it to the unauthenticated cluster join endpoint, and receive a service-scoped administrator token that is immediately exchangeable for a non-expiring full administrator platform token.

#3

Exploitation activity against the CVE-2026-42018 and CVE-2026-42016 chain was observed between August 15 and September 8, 2026, which places it after vendor fixes for CVE-2026-42018 had already shipped on the 7.146 branch in April and the 7.133 branch in August. CVE-2026-82329 was disclosed and patched on August 28, 2026; a public exploit appeared on September 1, and exploitation attempts climbed from single-digit probing to roughly 75,000 attempts on August 31, approximately 171,000 on September 1, and a peak of about 406,000 on September 2, originating from nearly 1,400 distinct source addresses in a single day. CISA added CVE-2026-82329 to the Known Exploited Vulnerabilities catalog on September 2, 2026, with a September 5 remediation deadline for federal civilian agencies.

#4

Post-exploitation activity has been consistent across intrusions and includes creation of administrator accounts under the "token: anonymous" actor identity, enumeration of repositories, users, and tokens, exfiltration of the system configuration and the cluster join key, installation of malicious Groovy plugins through Artifactory's own plugin framework, staging of webshells and binary droppers into world-writable directories such as /dev/shm, /tmp, and /var/tmp, addition of SSH keys to newly created accounts, and deployment of a custom rust-based backdoor with command-and-control capability, malicious Groovy plugins used as server-side backdoors that beacons to attacker infrastructure on non-standard ports.

#5

The business impact is severe and extends well beyond the Artifactory host itself, because an artifact repository is a trusted distribution point for the software that an organization builds and ships. Administrative control of Artifactory gives an attacker the ability to read every stored artifact, to modify or replace binaries, container images, and packages that downstream build systems and production estates will subsequently pull and execute, and to harvest the upstream registry, LDAP, proxy, and mail credentials held in the platform configuration. That combination converts a single unauthenticated network request into a viable software supply chain compromise affecting every consumer of the repository, and it does so with minimal noise, since the only consistently visible step in the observed intrusions is the repository, user and token enumeration that immediately follows access.

#6

The exposure does not end when the binary is patched. The administrator tokens minted through CVE-2026-82329 are issued with administrator scope and no expiration claim at all, and JFrog treats tokens as standalone credentials with a revocation path separate from the Access service lifecycle. Upgrading closes the route used to forge new tokens but leaves every previously issued token valid, so an organization that patches without enumerating and individually revoking long-lived administrator tokens, rotating the cluster join key and downstream secrets, and auditing accounts, SSH keys and Groovy plugins added since August 15 remains fully compromised while believing it has remediated. Scale compounds the problem, with reporting placing between 49 and 62 percent of reachable Artifactory instances vulnerable to at least one of the three flaws, and remediation of CVE-2026-42016 stalling near 59 percent still vulnerable more than six weeks after disclosure.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-42016	JFrog Artifactory Self-Hosted Before 7.133.11	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	CWE-863
CVE-2026-42018	JFrog Artifactory Self-Hosted Before 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.8	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	CWE-287
CVE-2026-82329	JFrog Artifactory Self-Hosted 7.111.4 to 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.37; 7.161.0 to 7.161.19	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	CWE-287

Recommendations

Upgrade Artifactory to a Fixed Build Immediately: Move every self-hosted Artifactory instance to 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38 or 7.161.20, whichever is the correct target for your release branch, or to a later build. This set of builds remediates all three vulnerabilities in this advisory, including CVE-2026-82329, which CISA required federal civilian agencies to remediate by September 5, 2026. JFrog Cloud instances are reported as unaffected and require no action, but any self-managed deployment reachable from the internet should be treated as urgent regardless of whether exploitation has been confirmed locally.

Assume Compromise and Revoke Every Long-Lived Administrator Token: Patching alone does not remediate this incident, because the administrator tokens minted through CVE-2026-82329 carry administrator scope with no expiration claim and survive the upgrade untouched. Enumerate all access tokens on the platform, identify every admin-scoped token that lacks an expiry claim, and revoke each one individually rather than assuming the upgrade invalidated them. Allow for token caching inside the platform, since revocation is not an instantaneous eviction and a revoked token may continue to be honoured briefly.

Establish the Exposure Window from Access Service Logs: Search the Access service startup logs for the key identifier prefix "kid: e3b0c442", which indicates that the empty-string join key was registered and the instance was exploitable. Then hunt for HTTP 201 responses returned from /access/api/v1/registry/join and its /router variants, particularly where the request originated from a node that is not a recognised member of the cluster. Together these two checks give a defensible start and end date for the exposure window and tell you whether forging was merely possible or actually succeeded.

Hunt the Chained Exploitation Pattern in Access Logs: Look for an HTTP 401 on a bare Access API path followed shortly by an HTTP 200 on a trailing-slash or otherwise altered variant of the same path from the same client, which is the signature of CVE-2026-42018. Correlate any such event with a subsequent POST to /access/api/v1/tokens from a low-privilege identity, and with administrator accounts created under the "token:anonymous" actor identity, which is the distinguishing artifact of the full chain. Treat a match as a confirmed intrusion rather than an exploitation attempt.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	
Persistence	T1136: Create Account	T1136.001: Local Account
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1505: Server Software Component	T1505.003: Web Shell
	T1053: Scheduled Task/Job	
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
Execution	T1059: Command and Scripting Interpreter	
Discovery	T1087: Account Discovery	
	T1083: File and Directory Discovery	
	T1589: Gather Victim Identity Information	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1550: Use Alternate Authentication Material	T1550.001: Application Access Tokens
Command and Control	T1105: Ingress Tool Transfer	
	T1571: Non-Standard Port	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	513a907b69edffc3cb77a494da395178d21ef9bd
IPv4	149[.]102[.]229[.]150, 186[.]247[.]79[.]240, 182[.]62[.]201[.]69, 146[.]19[.]216[.]120, 155[.]254[.]120[.]23, 137[.]184[.]111[.]69, 45[.]61[.]176[.]88, 185[.]190[.]58[.]172, 103[.]124[.]165[.]42, 176[.]88[.]121[.]152, 105[.]188[.]75[.]16, 223[.]144[.]227[.]110, 129[.]121[.]56[.]234, 104[.]28[.]251[.]139, 15[.]157[.]64[.]113, 16[.]54[.]250[.]190, 220[.]246[.]124[.]92, 213[.]136[.]72[.]87, 89[.]117[.]49[.]147, 45[.]33[.]75[.]219, 23[.]92[.]20[.]11, 173[.]255[.]226[.]148, 195[.]154[.]157[.]234, 62[.]210[.]87[.]212, 45[.]79[.]190[.]169, 163[.]172[.]132[.]245
IPv4:Port	64[.]207[.]232[.]6[:]8443
Domain	log[.]gitclone[.]org
URLs	hxxp[:]//log[.]gitclone[.]org[:]45678/smtp, hxxp[:]//3[.]88[.]162[.]79[:]36789/smtp
File Path	/tmp/.z, /dev/shm, /tmp, /var/tmp
HTTP Request	POST /access/api/v1/registry/join, POST /access/api/v1/registry/join/router

TYPE	VALUE
HTTP Request	POST /access/api/v1/registry/join/router?override=true, POST /access/api/v1/aws/token/, POST /access/api/v1/tokens, PUT /api/security/users/, GET /api/system/configuration, GET /access/api/security/tokens, GET /access/api/security/users, GET /access/api/v1/users
JWT Key ID	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Patch Link

https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

References

https://www.wiz.io/blog/artifactory-under-attack-in-the-wild-exploitation-of-cve-2026-42016-cve-2026-4201

https://www.fastly.com/blog/cve-2026-82329-jfrog-artifactory-authentication-bypass-exploitation-activity

https://mine2.io/blog/2026-09-13-artifactory-82329-tokens-outlive-the-patch/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 18, 2026 • 07:00 AM

More at www.hivepro.com