



THE LEAD / JFROG ARTIFACTORY

ARTIFACT REPOSITORIES: A NEW FRONT DOOR

Three chained flaws in self-hosted JFrog Artifactory handed attackers admin access to the systems that hold your builds, packages, and deployment secrets. Then the first week of October put three internet-facing appliances on the exploited list.

Threat actors are chaining three flaws in self-hosted JFrog Artifactory. The worst is CVE-2026-82329 (CVSS 9.8), an authentication bypass in JFrog Access, the component that issues and checks credentials. Under default configuration an instance with no extra join key gets a 'phantom' key, and anyone who can reach the server can use it to forge administrator credentials. watchTower saw attackers minting admin tokens as early as September 1.

The other two were chained from mid-August through September 8. CVE-2026-42018 leaks an anonymous-user token plus repository data. CVE-2026-42016 lets that low-value token climb to higher privilege because token validation is too loose. What followed: persistent admin accounts, malicious plugins, shell commands through plugin endpoints, stolen cluster keys, and attacker SSH keys on the host.

Artifact platforms sit next to source code, build outputs, and deployment pipelines. An admin foothold here turns a supply-chain control point into a persistence layer. Treat it as a build and credential incident, and remember the detail that matters most: patching does not revoke tokens minted before the fix.

IMMEDIATE ACTIONS

- **Inventory** every internet-facing and self-managed Artifactory instance, including the forgotten ones.
- **Patch** to the fixed branches in the JFrog advisory (7.111.21 through 7.161.20 by line).
- **Rotate** admin and repository tokens plus cluster keys, then audit who minted what.

AT A GLANCE

3 CVEs

chained for admin access in self-hosted Artifactory

9.8

CVSS on CVE-2026-82329, the JFrog Access auth bypass

Sep 1

earliest observed admin-token minting by attackers

KEV

all three listed in the CISA Known Exploited catalog

IN THIS ISSUE

02 Citrix, Fortinet, Cisco: three exploited edge flaws in one week

02 What to hunt for on appliances you already patched

03 Response plan, red-team tests, and end-of-year testing

EXPLOITATION WATCH / OCT 1-5

THE EDGE TOOK THREE HITS IN ONE WEEK

Artifactory was the supply-chain story. The first week of October was about internet-facing appliances: three vendors, three exploited flaws, one pattern. Here is what each one actually lets an attacker do.

NETSCALER / CVE-2026-88779

ZERO-DAY ON PATCHED APPLIANCES

Hits NetScaler ADC and Gateway configured as a SAML service provider or identity provider. Unauthenticated memory overflow; confirmed impact is denial of service, and it landed on appliances patched days earlier for CVE-2026-88771 and 88772. Responders saw shell commands stuffed into username fields and malware pulled onto honeypots. Fixed in 14.1-73.41 and 13.1-64.28.

FORTIMAIL / CVE-2026-104286

WRITE ANY FILE, NO LOGIN

A path traversal plus null-byte bug lets an attacker with no credentials write arbitrary files to the appliance through crafted HTTP requests. CVSS 9.8. Fortinet's own IOCs show the follow-through: a planted webconsole binary, an ld.so.preload hook, a modified httpd.conf. Until your branch is fixed: disable IBE and pull the admin UI off the internet.

SD-WAN MANAGER / CVE-2026-76504

ADMIN VIA A HEX-ENCODED URL

Catalyst SD-WAN Manager mishandles URI encoding, so a URL-encoded variant of /j_security_check skips authentication and reaches the API as the admin user. CVSS 9.8, exploited since September, and the eighth SD-WAN CVE on KEV this year. Hunt for j_security_check from unknown IPs and logins for users beginning viptela-reserved-.

WHAT TO HUNT ON THE EDGE

- **Crashes and reboots** on NetScaler paired with odd SAML authentication requests just before the outage.
- **Encoded login paths.** POSTs to URL-encoded forms of /j_security_check, and sessions for viptela-reserved-* users.
- **New binaries** under /data/bin on FortiMail, an ld.so.preload entry, or an edited httpd.conf.
- **Accounts and tokens created near the patch date** on any appliance or repository. Patching does not evict a token.
- **Outbound connections from the appliance itself.** Appliances almost never need to call out. When they do, ask why.

EXPOSURE SNAPSHOT

SURFACE	STATUS	PRIORITY
NetScaler with SAML	Exploited	Critical
FortiMail, IBE enabled	Exploited	Critical
SD-WAN Manager API	Exploited	Critical
Self-hosted Artifactory	Exploited	Critical
Zimbra, Check Point, F5 APM	Exploited	High



Internet-facing appliances rarely run EDR, rarely get forensic attention, and never get a day off. That is exactly why they keep getting hit.

uMercs field team

PRACTICAL VALIDATION

From the outside in: confirm which appliances and repository managers answer on the public internet, and whether their admin interfaces do too. Check versions against the Citrix, Fortinet, Cisco, and JFrog advisories, then prove the fix: retired tokens must fail, encoded login paths must 401, and the SAML preconditions on NetScaler must be known, not assumed.

Then go one layer down. Pull appliance logs and the artifacts built during each exploitation window and look for what the vendor IOCs describe. If an attacker held admin on the box that fronts your remote access or ships your software, the integrity question extends to everything behind it.

FIELD NOTES

A THREE-PART RESPONSE

Contain, scope, restore trust. In that order, whether the box is a repository manager or a gateway, and do not skip the middle step because the patch is already applied.

01

CONTAIN

Cut network reachability to trusted administration paths. Isolate any instance with credible indicators. Pull admin UIs off the internet immediately and keep them off; for FortiMail, disable IBE until your branch has a fix.

02

ESTABLISH SCOPE

Review administrator activity, tokens, plugins, SSH keys, new binaries, config changes, and every system the appliance can reach. Assume the attacker had time. Work the timeline backward from the first anomaly.

03

RESTORE TRUST

Patch to the vendor-fixed versions, rotate every secret the box could read, re-validate builds and sessions issued in the window, and watch for re-entry through the same path.

WHAT RED-TEAMERS SHOULD TEST

- **Discoverability.** Can your appliances and repository services be found from the public internet, and what does the banner or login page give away?
- **Authorization boundaries.** Does an encoded path, an anonymous token, or a SAML edge case travel further than it should?
- **Post-patch persistence.** After the fix, can a token minted before it still authenticate? Can a planted file survive a reboot?
- **Auditability.** In an authorized engagement, test whether defenders can see token minting, privilege changes, plugin activity, and new binaries. Exploitability is half the finding.

QUESTIONS FOR YOUR TEAM

- ☐ Do we know every appliance and artifact manager that faces the internet, and who owns each one?
- ☐ Who patches edge gear in an emergency, and how fast can they move on a Friday?
- ☐ Can we revoke appliance credentials and repository tokens without breaking production?
- ☐ Could we prove what shipped, or who logged in, during an exploitation window?
- ☐ When did someone last test these paths end to end?

THE DEBRIEF

BLUE TEAM: "Is the package repository patched?"

RED TEAM: "Yes. Are its tokens, plugins, and audit trail clean?"

Silence is also an answer. Just not the one you want in the status meeting.

END-OF-YEAR TESTING

BOOK BEFORE Q4 FILLS UP

Compliance deadlines do not slide. Lock in your penetration test now, before the calendar fills and your auditor comes knocking.

umercs.com

SOURCES

- CSO Online via daily.dev, "Exploited JFrog Artifactory bug puts software supply chain on alert" (Sep 2, 2026); SecurityWeek, "Three JFrog Artifactory Flaws Exploited for Backdoor Deployment"
- The Hacker News, "Critical FortiMail Zero-Day Flaw Exploited in Attacks" (Oct 2, 2026) and Fortinet advisory for CVE-2026-104286
- The Hacker News, "CISA Adds Exploited Cisco Catalyst SD-WAN Manager Auth Bypass to KEV" (Oct 1, 2026); Cisco advisory for CVE-2026-76504
- SOC Prime and SecurityWeek reporting on Citrix NetScaler CVE-2026-88779 (Oct 5, 2026); Citrix security bulletin
- CISA Known Exploited Vulnerabilities Catalog, entries for JFrog, Fortinet, Cisco, and Citrix