



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Monday, September 14, 2026

CAL-CSIC-202608-A-006

Critical Authentication Bypass Vulnerability Affecting JFrog Artifactory Under Active Exploitation

Authentication Bypass

Supply Chain Manipulation

Under Active Exploitation

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critically rated vulnerability identified in JFrog's Artifactory repository manager. Organizations use Artifactory to store and distribute binaries, packages, AI models, and other software artifacts. CVE-2026-82329 is an authentication bypass vulnerability that carries a CVSS 3.1 score of 9.8.¹

CVE-2026-82329 is an Authentication Bypass vulnerability that impacts unpatched Artifactory environments. The vulnerability allows attackers to circumvent authentication controls and gain administrator-level access. Successful exploitation can create opportunities for the attacker to conduct data theft and software supply-chain manipulation and lateral movement into production infrastructure. Additionally, an attacker could tamper with software packages, inject malicious code into build processes, and exfiltrate sensitive intellectual property.²

JFrog has acknowledged the vulnerability and has issued a security advisory with workaround, mitigation, and updating guidance that addresses CVE-2026-82329.³ JFrog is aware of exploitation attempts on unpatched Artifactory environments. JFrog has also stated that their cloud environments have already been fortified and that no action is required. Additionally, CVE-2026-82329 was placed in CISA's Known Exploited Vulnerabilities catalog.

The Cal-CSIC recommends following JFrog's mitigation and updating guidance as soon as possible.

For additional details regarding CVE-2026-82329 please use this link:

CVE-2026-0257 Security Advisory: [JFrog Security Advisories](#)

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Products and Versions⁴

Product	Affected Version	Unaffected Version
Artifactory	7.161.0 > 7.161.19	7.161.20
Artifactory	7.146.0 > 7.146.36	7.146.38
Artifactory	7.133.0 > 7.133.28	7.133.29
Artifactory	7.125.0 > 7.125.19	7.125.20
Artifactory	7.117.0 > 7.117.27	7.117.28
Artifactory	7.111.4 > 7.111.21	7.111.21

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

References

-
- ¹ OpenCVE; "CVE-2026-82329"; <https://app.opencve.io/cve/CVE-2026-82329>; accessed 14 September 2026
- ² SOCPrime; "CVE-2026-82329: Critical JFrog Artifactory Authentication Bypass Exploited in the Wild"; <https://socprime.com/blog/cve-2026-82329-analysis/>; accessed 14 September 2026
- ³ JFrog Docs; "JFrog Security Advisories"; <https://docs.jfrog.com/releases/docs/jfrog-security-advisories#cve-2026-82329---potential-authentication-bypass-leading-to-administrative-access-in-artifactory>; accessed 14 September 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR