SECURITY ADVISORIES

JFrog Security Advisories

JFrog security advisories and CVE information for Artifactory vulnerabilities, with detailed information on affected versions and remediation guidance.

Support

For support inquiries, visit JFrog Support.

JFrog takes the privacy and security of its customers very seriously and always strives to provide prompt notification and remediation of any vulnerabilities discovered on JFrog products. As a CVE Numbering Authority (CNA), JFrog assigns CVE identification numbers to newly discovered security vulnerabilities.

Security Advisories

Severity	CVE	Summary	Product	Versions	Published	Updated
Critical	CVE-2026-82329	Potential authentication bypass leading to administrative access in Artifactory.	Artifactory	7.161.0 > 7.161.19 7.146.0 > 7.146.36 7.133.0 > 7.133.28 7.125.0 > 7.125.19 7.117.0 > 7.117.27 7.111.4 > 7.111.21	28 Aug 2026	28 Aug 2026
High	CVE-2026-70551	Server-Side Request Forgery Via VCS remote download in JFrog Artifactory.	Artifactory	7.161.0 > 7.161.16 7.146.0 > 7.146.35	25 Aug 2026	25 Aug 2026
Medium	CVE-2026-70550	An authorization weakness in JFrog Artifactory Composer repository handling may allow an authenticated user to read package metadata from repositories they are not authorized to read.	Artifactory	7.161.0 > 7.161.11 7.146.0 > 7.146.35	25 Aug 2026	25 Aug 2026
Low	CVE-2026-70548	Under specific circumstances, low-level user can run request to remote CocoaPods repos via JFrog Artifactory External Dependency	Artifactory	7.161.0 > 7.161.1 7.161.11 > 7.161.16 7.146.0 > 7.146.29	25 Aug 2026	25 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
High	CVE-2026-69104	An authenticated user may initiate repository migration operations without required repository permissions.	Artifactory	7.161.0 > 7.161.18	25 Aug 2026	25 Aug 2026
Medium	CVE-2026-70547	An authenticated user without repository read permission may access package metadata.	Artifactory	7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026
High	CVE-2026-69105	An unauthenticated attacker may cause untrusted package content to be cached, affecting artifact integrity and availability.	Artifactory	7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026
Medium	CVE-2026-69107	An unauthenticated user may access restricted artifacts under specific conditions.	Artifactory	< 7.104.16; 7.111.0 –>7.111.14; 7.117.0 –> 7.117.21; 7.125.0 -> 7.125.14; 7.133.0 –> 7.133.21; 7.146.0 –> 7.146.8	12 Aug 2026	12 Aug 2026
High	CVE-2026-69106	A low-privileged user may poison cached artifact metadata, potentially causing retrieval	Artifactory	<7.146.28	12 Aug 2026	13 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
		of untrusted content.				
High	CVE-2026-42018	Artifactory could return an internal anonymous-user token to an unauthenticated caller when anonymous access is disabled.	Artifactory	< 7.111.20; 7.117.0 –> 7.117.27; 7.125.0 –> 7.125.19; 7.133.0 –> 7.133.28; 7.146.0 –> 7.146.8	12 Aug 2026	13 Aug 2026
Medium	CVE-2026-66384	An authenticated user may write data outside the intended Docker cache path under specific remote-repository conditions.	Artifactory	<7.146.35; 7.161.0 -> 7.161.16	12 Aug 2026	12 Aug 2026
High	CVE-2026-66375	A low-privilege authenticated user may permanently remove protected internal metadata across repositories.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66016	Generated TLS private keys may be retained in rendered Helm manifests accessible to highly privileged local users.	Artifactory	< 7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Low	CVE-2026-65926	An anonymous or low-privilege user may learn private Release Bundle	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
		names and versions when the bundle name is known.				
Medium	CVE-2026-68760	An unauthenticated user may bypass authentication under specific cache conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66378	An authenticated user without repository read permission may access private NuGet metadata.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026
Medium	CVE-2026-66380	An authenticated user without repository read permission may access private OCI referrer metadata.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66381	A repository reader with cache-deploy permission may access content outside a configured upstream path.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66382	An authenticated user may write files outside the intended Artifactory work directory.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66376	Credentials for a deleted user may remain valid for a short period	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
		under specific conditions.				
Medium	CVE-2026-68754	A repository publisher without delete permission may modify protected package content.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
High	CVE-2026-68757	A user with access to a valid SAML response may impersonate another user under specific conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-68756	A party with write access to stored session data may affect Artifactory under specific conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026
High	CVE-2026-68752	A Project Resource Manager may gain broader administrative privileges under specific conditions.	Artifactory	< 7.146.35	12 Aug 2026	13 Aug 2026
Medium	CVE-2026-68755	A bundle writer may create misleading release-promotion information under specific conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
Medium	CVE-2026-68753	An unauthenticated user may access restricted content when a credentialed remote repository is configured in a specific way.	Artifactory	< 7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
High	CVE-2026-68759	A holder of a valid integration credential may impersonate other users under specific conditions.	Artifactory	< 7.146.35; 7.161.0–> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-68758	A low-privileged authenticated user may access restricted support information under specific conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	12 Aug 2026
Medium	CVE-2026-66377	An unauthenticated user may access restricted repository information under specific conditions.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026
Medium	CVE-2026-66379	An authenticated user may view private Puppet module metadata without repository read access.	Artifactory	<7.146.35; 7.161.0 –> 7.161.16	12 Aug 2026	13 Aug 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
Medium	CVE-2026-65924	Terraform remote repositories could issue outbound requests to arbitrary destinations and return response content.	Artifactory	<7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
High	CVE-2026-66015	An authenticated authorization flaw may grant temporary platform administrator access.	Artifactory	7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
High	CVE-2026-66014	An internal request authentication weakness may allow privilege escalation under specific conditions.	Artifactory	<7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
Medium	CVE-2026-66018	Build readers can access another repository's environment properties, potentially exposing build secrets.	Artifactory	7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
Medium	CVE-2026-65923	An Ansible repository URL-validation weakness could	Artifactory	< 7.111.18; 7.117.0–> 7.117.25;	27 Jul 2026	27 Jul 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
		cause unintended server-side requests.		7.125.0–> 7.125.18; 7.133.0–> 7.133.27; 7.146.0–> 7.146.34; 7.161.0–> 7.161.15		
High	CVE-2026-65922	An authorization weakness could let a limited repository user write to restricted internal metadata areas.	Artifactory	<7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
High	CVE-2026-65921	Archive path validation allows traversal entries to be written outside the intended build-artifacts location.	Artifactory	< 7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
Medium	CVE-2026-65925	A user with Cargo remote-repository read access could make Artifactory request unintended URLs and return the response.	Artifactory	< 7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
High	CVE-2026-65617	A package-handling deserialization weakness could let a low-privileged user affect confidentiality, integrity, and availability.	Artifactory	< 7.111.18; 7.117.0 –> 7.117.25; 7.125.0 –> 7.125.18; 7.133.0 –> 7.133.27; 7.146.0 –> 7.146.34; 7.161.0 –> 7.161.15	27 Jul 2026	27 Jul 2026
High	CVE-2026-65616	Incorrect refresh-token signature validation allows non-admin users to obtain a signed administrator token.	Artifactory	< 7.146.27	27 Jul 2026	27 Jul 2026
High	CVE-2026-42017	An event-handling weakness could expose privileged authorization material to a lower-privileged user.	Artifactory	< 7.133.21; 7.146.0 –> 7.146.8	27 Jul 2026	27 Jul 2026
High	CVE-2026-42016	JFrog Artifactory (Self Hosted) versions before 7.133.11 are vulnerable to a privilege escalation attack due to a validation check of the token signature/issuer and not the token's scope.	Artifactory	<7.133.11	27 Jul 2026	27 Jul 2026

Severity	CVE	Summary	Product	Versions	Published	Updated
Medium	CVE-2026-65618	Improper URL validation when handling specific URLs allows unauthorized requests from Artifactory, potentially exposing internal services and cached response data.	Artifactory	<7.133.6	27 Jul 2026	27 Jul 2026
Medium	CVE-2025-14830	JFrog Artifactory is vulnerable to improper handling of import Validation Mechanism which could lead to DOM-based cross-site scripting.	Artifactory	Artifactory Self Hosted < 7.94.0 > 7.117.10	4 Jan 26	4 Jan 26
Critical	CVE-2024-6915	JFrog Artifactory is vulnerable to Improper Input Validation that could potentially lead to Cache Poisoning.	Artifactory	Artifactory Self Hosted < 7.90.6, < 7.84.20, < 7.77.14, < 7.71.23, < 7.68.22, < 7.63.22, < 7.59.23, < 7.55.18	5 Aug 24	5 Aug 24
Medium	CVE-2024-2248	A Header Injection vulnerability in the JFrog platform may allow threat actors to take over the end user's account when clicking on a specially crafted URL sent to the	Artifactory	SaaS versions prior to 7.85.0, Self-Hosted version prior to 7.84.7	15 May 24	15 May 24

Severity	CVE	Summary	Product	Versions	Published	Updated
		victim's user email.				
Critical	CVE-2024-4142	An Improper input validation vulnerability was discovered in JFrog Artifactory. Due to this vulnerability, users with low privileges may gain administrative access to the system, an issue that could potentially lead to privilege escalation. This issue can also be exploited in Artifactory platforms with anonymous access enabled.	Artifactory	Artifactory Self-Hosted < 7.55.17, < 7.59.22, < 7.63.21, < 7.68.21, < 7.71.21, < 7.77.11; Artifactory Cloud < 7.84.6	1 May 24	1 May 24
Medium	CVE-2024-3505	JFrog Artifactory Self-Hosted versions prior to 7.77.3 are vulnerable to sensitive information disclosure whereby a low-privileged authenticated user can read the proxy configuration. This does not affect JFrog cloud deployments.	Artifactory	Self-hosted versions prior to 7.77.3	11 Apr 24	11 Apr 24
High	CVE-2024-	JFrog Artifactory prior to version	Artifactory	Versions prior to	13 Mar 24	13 Mar 24

Severity	CVE	Summary	Product	Versions	Published	Updated
	2247	7.77.7, is vulnerable to DOM-based cross-site scripting due to improper handling of the import override mechanism.		7.77.7		
High	CVE-2023-42661	JFrog Artifactory prior to version 7.76.2 is vulnerable to Arbitrary File Write of untrusted data, which may lead to DoS or Remote Code Execution when a specially crafted series of requests is sent by an authenticated user. This is due to insufficient validation of artifacts.	Artifactory	Versions prior to 7.76.2	7 Mar 24	7 Mar 24
Medium	CVE-2023-42509	JFrog Artifactory later than version 7.17.4 and prior to version 7.77.0 is vulnerable to an issue whereby a sequence of improperly handled exceptions in repository configuration initialization steps may lead to exposure of sensitive data.	Artifactory	Versions later than 7.17.4 but prior to version 7.77.0	7 Mar 24	7 Mar 24
Critical	CVE-2023-	JFrog Artifactory versions 7.59 and	Artifactory	Versions later than	6 Mar 24	6 Mar 24

Severity	CVE	Summary	Product	Versions	Published	Updated
	42662	above, but below 7.59.18, 7.63.18, 7.68.19, 7.71.8 are vulnerable to an issue whereby user interaction with specially crafted URLs could lead to exposure of user access tokens due to improper handling of the CLI / IDE browser based SSO integration.		7.59 but prior to: 7.59.18, 7.63.18, 7.68.19, 7.71.8		
Medium	CVE-2023-42508	JFrog Artifactory prior to version 7.66.0, is vulnerable to specific endpoint abuse with a specially crafted payload, which can lead to unauthenticated users being able to send emails with manipulated email body.	Artifactory	Versions prior to 7.66.0	10/04/2023	10/04/2023
Medium	CVE-2022-0668	JFrog Artifactory prior to versions 7.37.13 and 6.23.41. is vulnerable to Authentication Bypass, which can lead to Privilege Escalation when a specially crafted request is sent by an unauthenticated user.	Artifactory	Versions prior to 7.37.13, Versions prior to 6.23.41	01/02/2023	01/02/2023

Severity	CVE	Summary	Product	Versions	Published	Updated
Medium	CVE-2021-45721	JFrog Artifactory prior to version 7.29.8 and 6.23.38is vulnerable to Reflected Cross-Site Scripting (XSS) through one of the XHR parameters in the Users REST API endpoint.	Artifactory	Versions prior to 7.29.8, Versions prior to 6.23.38	07/05/2022	07/05/2022
Medium	CVE-2021-46687	JFrog Artifactory prior to version 7.31.10and 6.23.38is vulnerable to Sensitive Data Exposure through the Project Administrator REST API.	Artifactory	Versions prior to 7.31.10, Versions prior to 6.23.38	07/05/2022	07/05/2022
Low	CVE-2021-23163	JFrog Artifactory prior to version 7.33.6 and 6.23.38, is vulnerable to CSRF (Cross-Site Request Forgery) for specific endpoints.	Artifactory	Versions prior to 7.33.6, Versions prior to 6.23.38	07/05/2022	07/05/2022
Medium	CVE-2021-41834	JFrog Artifactory prior to versions 7.28.0 and 6.23.38, is vulnerable to Broken Access Control, a low-privileged user can use the copy function to read and copy any artifact that exists	Artifactory	Versions prior to 7.28.0, Versions prior to 6.23.38	05/18/2022	05/18/2022

Severity	CVE	Summary	Product	Versions	Published	Updated
		in the Artifactory deployment due to improper permissions validation.				
Medium	CVE-2021-45730	JFrog Artifactory prior to 7.31.10, is vulnerable to Broken Access Control where a Project Admin is able to create, edit and delete Repository Layouts while Repository Layouts configuration should only be available for Platform Administrators.	Artifactory	Versions prior to 7.31.10	05/18/2022	05/18/2022
High	CVE-2022-0573	JFrog Artifactory prior to 7.36.1 and 6.23.41, is vulnerable to Insecure Deserialization of untrusted data which can lead to DoS, Privilege Escalation, and Remote Code Execution when a specially crafted request is sent by a low privileged authenticated user due to insufficient validation of a user-provided serialized object.	Artifactory	Versions prior to 7.36.1, Versions prior to 6.34.41	05/12/2022	05/12/2022

Severity	CVE	Summary	Product	Versions	Published	Updated
Low	CVE-2021-46270	JFrog Artifactory prior to 7.31.10, is vulnerable to Broken Access Control where a project admin user is able to list all available repository names due to insufficient permission validation.	Artifactory	Versions prior to 7.31.10	03/02/2022	03/02/2022
Medium	CVE-2021-45074	JFrog Artifactory prior to7.29.3 and 6.23.38, is vulnerable to Broken Access Control, a low-privileged user is able to delete other known users'OAuthtoken, which will force a reauthentication on an active session or in the following UI session.	Artifactory	Versions prior to 7.29.3, Versions prior to 6.23.38	03/02/2022	03/02/2022
High	CVE-2021-3860	JFrog Artifactory prior to version 7.25.4 (Enterprise+ deployments only), is vulnerable to Blind SQL Injection by a low privileged authenticated user due to incomplete validation when performing an SQL query.	Artifactory	Versions prior to 7.25.4, Versions prior to 6.23.30	12/15/2021	12/15/2021

CVE-2026-82329 - Potential authentication bypass leading to administrative access in Artifactory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-82329	Critical	CWE-287 Improper Authentication	28 Aug 2026	28 Aug 2026

Description

JFrog Artifactory contains an authentication weakness that, under default configuration, may allow an unauthenticated attacker with network access to obtain administrative privileges.

Affected Products

Product	Affected Versions	Patched 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

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, 7.161.20

Workarounds and Mitigations

The best known remediation is to upgrade to the patched version above.

However, if you are unable to upgrade rapidly, we recommend the following workaround to reduce risk to your systems.

An additional join key is a random, hex-encoded value in the same format as your join key. Generate one with any of the following:

Shell

```
# Option A: OpenSSL (recommended)
openssl rand -hex 16

# Option B: Python
python3 -c "import secrets; print(secrets.token_hex(16))"
```

Example output (do **not** reuse this — generate your own): `3f8c1a9b0d2e4f6a7b8c9d0e1f2a3b4c`

Keep this value secret, the same way you protect your join key.

To apply it:

1. Edit your `system.yaml` and add the generated `additionalJoinKeys` value under `shared › security`:

   Shell

   ```
   shared:
     security:
       ## Existing join key stays as-is; just add the line below.
       ## Use a strong, random value in the same format as your join key.
       additionalJoinKeys: "<your-strong-random-join-key-value>"
   ```

   - If you already have entries under `shared: security` : (for example, `joinKey`), keep them and simply add the `additionalJoinKeys` line — do not duplicate the `shared:` or `security:` headings.
   - For more than one key, use a comma-separated list: `additionalJoinKeys: "key1,key2"`
   - Containerized / Helm deployments can set the equivalent environment variable instead: `JF_SHARED_SECURITY_ADDITIONALJOINKEYS` .

2. Restart the Access service (or the JPD) for the change to take effect.

This workaround is designed to enforce that only your own keys are accepted for service registration. Your existing join key continues to work, so cluster operation is unaffected.

CVE-2026-70551 - Server-Side Request Forgery Via VCS Remote Download

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-70551	High	CWE-918 - Server-Side Request Forgery (SSRF)	25 Aug 2026	25 Aug 2026

Description

A user who can read an existing remote VCS repository can replace its configured origin or supply an absolute VCS data URL.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 > 7.161.17	7.161.19
Artifactory	7.146.0 > 7.146.35	7.146.36

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.19 or 7.146.36.

CVE-2026-70550 - Potential unauthorized access to private Composer repository metadata in JFrog Artifactory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-70550	Medium	CWE-862 Missing Authorization	25 Aug 2026	25 Aug 2026

Description

An authorization weakness in JFrog Artifactory Composer repository handling may allow an authenticated user, under specific conditions, to read package metadata from repositories they are not authorized to read. The issue affects confidentiality and has been addressed in fixed Artifactory versions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 > 7.161.11	7.161.19
Artifactory	0 > 7.146.29	7.146.36

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.19 or 7.146.36.

CVE-2026-70548 - SSRF In CocoaPods Via JFrog Artifactory External Dependency

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-70548	Low	CWE-918 - Server-Side Request Forgery (SSRF)	25 Aug 2026	25 Aug 2026

Description

Under specific circumstances, low-level user can run request to remote CocoaPods repos via JFrog Artifactory External Dependency.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 > 7.161.1	7.161.19
Artifactory	7.161.11 > 7.161.16	7.161.19
Artifactory	7.146.0 > 7.146.29	7.146.36

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.19 or 7.146.36.

CVE-2026-69104 - Potential unauthorized repository migration in JFrog Artifactory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-69104	High	CWE-862 Missing Authorization	25 Aug 2026	25 Aug 2026

Description

An authenticated user may initiate repository migration operations without required repository permissions, potentially causing partial information disclosure, unauthorized state changes, and service disruption. Fixed versions address the issue.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 > 7.161.18	7.161.19

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.19.

CVE-2026-70547 - Potential Unauthorized Metadata Exposure

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-70547	Medium	CWE-862 Missing Authorization	12 Aug 2026	13 Aug 2026

Description

An authenticated user without repository read permission may access package metadata.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.16.

CVE-2026-69105 - Potential Package Cache Integrity Issue

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-69105	High	CWE-345 Insufficient Verification of Data Authenticity	12 Aug 2026	13 Aug 2026

Description

An unauthenticated attacker may cause untrusted package content to be cached, affecting artifact integrity and availability.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.161.0 -> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.161.16.

CVE-2026-69107 - Potential Unauthorized Artifact Access

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-69107	Medium	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

An unauthenticated user may access restricted artifacts under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.104.16	7.104.16
Artifactory	7.111.0 –> 7.111.14	7.111.14
Artifactory	7.117.0 –> 7.117.21	7.117.21
Artifactory	7.125.0 –> 7.125.14	7.125.14
Artifactory	7.133.0 –> 7.133.21	7.133.21
Artifactory	7.146.0 –> 7.146.8	7.146.8

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.

- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.104.16, 7.111.14, 7.117.21, 7.125.14, 7.133.21, 7.146.8.

CVE-2026-69106 - Potential Cache Poisoning in JFrog Artifactory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-69106	High	CWE-20 Improper Input Validation	12 Aug 2026	13 Aug 2026

Description

A low-privileged user may poison cached artifact metadata, potentially causing retrieval of untrusted content.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.28	7.146.28

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.28.

CVE-2026-42018 - Anonymous User Token Generation Exposure

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-42018	High	CWE-287 Improper Authentication	12 Aug 2026	13 Aug 2026

Description

Artifactory could return an internal anonymous-user token to an unauthenticated caller when anonymous access is disabled.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.111.20	7.111.20
Artifactory	7.117.0–>7.117.27	7.117.27
Artifactory	7.125.0–>7.125.19	7.125.19
Artifactory	7.133.0–>7.133.28	7.133.28
Artifactory	7.146.0–>7.146.8	7.146.8

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.20, 7.117.27, 7.125.19, 7.133.28, 7.146.8.

CVE-2026-66384 - Authenticated Users May Write Data Outside the Intended Docker Cache Path

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66384	Medium	CWE-22 Improper Limitation of a Pathname to a Restricted Directory	12 Aug 2026	12 Aug 2026

Description

An authenticated user may write data outside the intended Docker cache path under specific remote-repository conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0–> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66375 - Low-Privilege Users May Remove Protected Artifactory Metadata

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66375	High	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

A low-privilege authenticated user may permanently remove protected internal metadata across repositories.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66016 - Rendered Helm Manifests May Contain Generated TLS Private Keys

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66016	Medium	CWE-312 Cleartext Storage of Sensitive Information	12 Aug 2026	12 Aug 2026

Description

Generated TLS private keys may be retained in rendered Helm manifests accessible to highly privileged local users.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-65926 - Private Release Bundle Versions May Be Disclosed

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65926	Low	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

An anonymous or low-privilege user may learn private Release Bundle names and versions when the bundle name is known.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68760 - Potential Remember-Me Authentication Bypass

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68760	Medium	CWE-287 Improper Authentication	12 Aug 2026	12 Aug 2026

Description

An unauthenticated user may bypass authentication under specific cache conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66378 - Authenticated Users May Access Private NuGet Metadata

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66378	Medium	CWE-862 Missing Authorization	12 Aug 2026	13 Aug 2026

Description

An authenticated user without repository read permission may access private NuGet metadata.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66380 - Authenticated Users May Access Private OCI Referrer Metadata

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66380	Medium	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

An authenticated user without repository read permission may access private OCI referrer metadata.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66381 - Repository Readers May Access Content Outside Configured Upstream Paths

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66381	Medium	CWE-22 Improper Limitation of a Pathname to a Restricted Directory	12 Aug 2026	12 Aug 2026

Description

A repository reader with cache-deploy permission may access content outside a configured upstream path.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66382 - Authenticated Users May Write Files Outside the Intended Work Directory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66382	Medium	CWE-22 Improper Limitation of a Pathname to a Restricted Directory	12 Aug 2026	12 Aug 2026

Description

An authenticated user may write files outside the intended Artifactory work directory.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66376 - Deleted Users May Temporarily Retain Access

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66376	Medium	CWE-613 Insufficient Session Expiration	12 Aug 2026	12 Aug 2026

Description

Credentials for a deleted user may remain valid for a short period under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68754 - Publishers Without Delete Permission Can Overwrite Docker Layer Information

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68754	Medium	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

A repository publisher without delete permission may modify protected package content.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68757 - Potential Improper SAML Signature Verification

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68757	High	CWE-347 Improper Verification of Cryptographic Signature	12 Aug 2026	12 Aug 2026

Description

A user with access to a valid SAML response may impersonate another user under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68756 - Potential Insecure Deserialization in JFrog Artifactory

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68756	Medium	CWE-502 Deserialization of Untrusted Data	12 Aug 2026	13 Aug 2026

Description

A party with write access to stored session data may affect Artifactory under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68752 - Project Resource Managers May Escalate Privileges

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68752	High	CWE-269 Improper Privilege Management	12 Aug 2026	13 Aug 2026

Description

A Project Resource Manager may gain broader administrative privileges under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35.

CVE-2026-68755 - Bundle Writers May Alter Trusted Release Information

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68755	Medium	CWE-863 Incorrect Authorization	12 Aug 2026	12 Aug 2026

Description

A bundle writer may create misleading release-promotion information under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68753 - Anonymous Users May Access Restricted Content Under Specific Configurations

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68753	Medium	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

An unauthenticated user may access restricted content when a credentialed remote repository is configured in a specific way.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68759 - Integration Credential Holders May Impersonate Users

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68759	High	CWE-347 Improper Verification of Cryptographic Signature	12 Aug 2026	12 Aug 2026

Description

A holder of a valid integration credential may impersonate other users under specific conditions.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-68758 - Authenticated Users May Access Restricted Support Information

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-68758	Medium	CWE-862 Missing Authorization	12 Aug 2026	12 Aug 2026

Description

A low-privileged authenticated user may access restricted support information under specific conditions.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66377 - Anonymous Users May Access Restricted Repository Information

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66377	Medium	CWE-862 Missing Authorization	12 Aug 2026	13 Aug 2026

Description

An unauthenticated user may access restricted repository information under specific conditions.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-66379 - Authenticated Users May View Private Puppet Module Metadata

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66379	Medium	CWE-862 Missing Authorization	12 Aug 2026	13 Aug 2026

Description

An authenticated user may view private Puppet module metadata without repository read access.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.146.35	7.146.35
Artifactory	7.161.0 –> 7.161.16	7.161.16

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.35, 7.161.16.

CVE-2026-65924 - Server-Side Request Forgery via Terraform Remote Repository

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65924	Medium	CWE-918 Server-Side Request Forgery (SSRF)	27 Jul 2026	27 Jul 2026

Description

Terraform remote repositories could issue outbound requests to arbitrary destinations and return response content.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-66015 - Authorization Flaw May Allow Authenticated Privilege Escalation

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66015	High	CWE-269 Improper Privilege Management	27 Jul 2026	27 Jul 2026

Description

An authenticated authorization flaw may grant temporary platform administrator access.

Affected Products

Product	Affected Versions	Patched Version
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.34, 7.161.15.

CVE-2026-66014 - Potential Authentication Bypass Leading to Privilege Escalation

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66014	High	CWE-287 Improper Authentication	27 Jul 2026	27 Jul 2026

Description

An internal request authentication weakness may allow privilege escalation under specific conditions.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-66018 - JFrog Artifactory Build Environment Properties Exposure

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-66018	Medium	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	27 Jul 2026	27 Jul 2026

Description

Build readers can access another repository's environment properties, potentially exposing build secrets.

Affected Products

Product	Affected Version	Patched Version
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.34, 7.161.15.

CVE-2026-65923 - Potential SSRF in Artifactory Ansible Repository Handling

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65923	Medium	CWE-918 Server-Side Request Forgery (SSRF)	27 Jul 2026	27 Jul 2026

Description

An Ansible repository URL-validation weakness could cause unintended server-side requests.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-65922 - Potential Unauthorized Modification of Artifactory Internal Metadata

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65922	High	CWE-862 Missing Authorization	27 Jul 2026	27 Jul 2026

Description

An authorization weakness could let a limited repository user write to restricted internal metadata areas.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-65921 - Potential Path Traversal Leading to Unauthorized File Writes

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65921	High	CWE-22 Improper Limitation of a Pathname to a Restricted Directory	27 Jul 2026	27 Jul 2026

Description

Archive path validation allows traversal entries to be written outside the intended build-artifacts location.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0–<7.125.18	7.125.18
Artifactory	7.133.0–<7.133.27	7.133.27
Artifactory	7.146.0–<7.146.34	7.146.34
Artifactory	7.161.0–<7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-65925 - Server-Side Request Forgery via Artifactory Cargo Remote Repository

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65925	Medium	CWE-918 Server-Side Request Forgery (SSRF)	27 Jul 2026	27 Jul 2026

Description

A user with Cargo remote-repository read access could make Artifactory request unintended URLs and return the response.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-65617 - Potential Remote Code Execution on an Artifactory Package Service Container

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65617	High	CWE-502 Deserialization of Untrusted Data	27 Jul 2026	27 Jul 2026

Description

A package-handling deserialization weakness could let a low-privileged user affect confidentiality, integrity, and availability.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.111.18	7.111.18
Artifactory	7.117.0 –> 7.117.25	7.117.25
Artifactory	7.125.0 –> 7.125.18	7.125.18
Artifactory	7.133.0 –> 7.133.27	7.133.27
Artifactory	7.146.0 –> 7.146.34	7.146.34
Artifactory	7.161.0 –> 7.161.15	7.161.15

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.111.18, 7.117.25, 7.125.18, 7.133.27, 7.146.34, 7.161.15.

CVE-2026-65616 - Potential Privilege Escalation to JFrog Administrator Privileges

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65616	High	CWE-347 Improper Verification of Cryptographic Signature	27 Jul 2026	27 Jul 2026

Description

Incorrect refresh-token signature validation allows non-admin users to obtain a signed administrator token.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.146.27	7.146.27

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.146.27.

CVE-2026-42017 - Privilege Escalation via JFrog Worker Event Token Exposure

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-42017	High	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	27 Jul 2026	27 Jul 2026

Description

An event-handling weakness could expose privileged authorization material to a lower-privileged user.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.133.21	7.133.21
Artifactory	7.146.0 –> 7.146.8	7.146.8

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.133.21, 7.146.8.

CVE-2026-42016 - Incorrect User Token Authorization Validation Allows Privilege Escalation

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-42016	High	CWE-863 Incorrect Authorization	27 Jul 2026	27 Jul 2026

Description

JFrog Artifactory (Self Hosted) versions before 7.133.11 are vulnerable to a privilege escalation attack due to a validation check of the token signature/issuer and not the token’s scope.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.133.11	7.133.11

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.133.11.

CVE-2026-65618 - Improper URL Validation May Lead to SSRF

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2026-65618	Medium	CWE-918 Server-Side Request Forgery (SSRF)	27 Jul 2026	27 Jul 2026

Description

Improper URL validation when handling specific URLs allows unauthorized requests from Artifactory, potentially exposing internal services and cached response data.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.133.6	7.133.6

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade JFrog Artifactory to a fixed version applicable to your release branch: 7.133.6.

CVE-2025-14830 - Improper Handling of Import Validation Mechanism Could Lead to DOM-based Cross-site Scripting

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2025-14830	Medium	CWE-79 Improper Authentication	January 4, 2026	January 4, 2026

Description

JFrog Artifactory versions later than 7.94.0 but prior to version 7.117.10 (Enterprise+ and Enterprise X deployments only), are vulnerable to DOM-based cross-site scripting due to improper handling of the import validation mechanism.

Affected Products

Product	Affected Version	Patched Version
Artifactory	Versions greater than 7.94.0 but less than 7.117.10	7.117.10

How to Fix

- **Cloud Environment**: Affected Cloud environments have already been fortified. No action is required for cloud instances.
- **Self-Hosted Environment**: Upgrade to version 7.117.10

Workarounds and Mitigations

Users can block the Workers functionality:

- Block /ui/admin/workers/ path on WAF
- Uninstall Workers

CVE-2024-6915 - Cache Poisoning

CVE Identifier	Severity	CWE Weakness Type	Date Published	Date Updated
CVE-2024-6915	Critical	CWE-20	August 5, 2024	August 5, 2024

Description

JFrog Artifactory versions below 7.90.6, 7.84.20, 7.77.14, 7.71.23, 7.68.22, 7.63.22, 7.59.23, and 7.55.18 are vulnerable to Improper Input Validation that could potentially lead to Cache Poisoning.

Affected Products

Product	Affected Version	Patched Version
Artifactory	< 7.90.6	7.90.6
Artifactory	< 7.84.20	7.84.20
Artifactory	< 7.77.14	7.77.14
Artifactory	< 7.71.23	7.71.23
Artifactory	< 7.68.22	7.68.22
Artifactory	< 7.63.22	7.63.22
Artifactory	< 7.59.23	7.59.23
Artifactory	< 7.55.18	7.55.18

How to Fix

- **Self Hosted**: To fix this issue, upgrade using the security patch for your required Patched Version from the following location: https://jfrog.com/download-legacy/
- **Cloud**:
  - Environments have already been updated to a fixed version containing additional security controls. No action is required for cloud instances.
  - Cloud customers with Hybrid deployments where their Edge resides on-premise will need to upgrade their on-premise Edge instance

Workarounds and Mitigations

Disable anonymous access or remove Deploy/Cache permissions for remote repositories for the Anonymous account.

Acknowledgements

This issue was discovered and reported by **Michael Stepankin (artsploit)** from **GitHub Security Lab**.

CVE-2024-2248 - JFrog Artifactory Header Injection

CVE Identifier	Severity	CWE / Weakness Type	Date Publishing	Date Updated
CVE-2024-2248	Medium	CWE-20 Exposure of Sensitive Information to an Unauthorized Actor	15 May 24	15 May 24

Description

A Header Injection vulnerability in the JFrog platform in versions below 7.85.0 (SaaS) and 7.84.7 (Self-Hosted) may allow threat actors to take over the end user's account when clicking on a specially crafted URL sent to the victim's user email.

Affected Products

Product	Affected Version	Patched Version
Artifactory SaaS	< 7.85.0	7.85.0
Artifactory Self-Hosted	< 7.84.7	7.84.7

How to Fix

- **Cloud Environments**: JFrog Cloud environments are protected against this vulnerability with a deployed version containing the fix.
- **Self-Hosted Environments**: To fix this issue, take the following action. Upgrade your version of Artifactory to one of the versions listed above.

Workarounds and Mitigations

No workarounds.

Acknowledgements

This issue was discovered and reported by the researcher Master Hackor via HackerOne.

CVE-2024-4142 - Improper Input Validation in Artifactory Token Creation Flow

Critical security vulnerability CVE-2024-4142 affecting JFrog Artifactory with improper input validation that could lead to privilege escalation.

CVE ID	Severity	CWE / Weakness Type	Date Published	Date Updated
CVE-2024-4142	Critical	CWE-20 Improper Input Validation		1 May 24

Description

An Improper input validation vulnerability was discovered in JFrog Artifactory. Due to this vulnerability, users with low privileges may gain administrative access to the system, an issue that could potentially lead to privilege escalation.

This issue can also be exploited in Artifactory platforms with anonymous access enabled.

Affected Products

Product	Affected Version	Patched Versions
Artifactory Self-Hosted	<7.55.17 <7.59.22 <7.63.21 <7.68.21 <7.71.21 <7.77.11	7.55.17 7.59.22 7.63.21 7.68.21 7.71.21 7.77.11
Artifactory Cloud	<7.84.6	7.84.6

How to Fix

- **Cloud environments**: No action is required for Cloud environments: the affected environments have already been protected.
- **Self-Hosted environments**: Update to one of the provided patched/ fixed versions listed above.

To apply the security fix, you must upgrade your version of JFrog Artifactory to one of the remediating versions.

To download and install remediating versions, click here. Please ensure that you select the correct patch for your current installation from the Product Version drop-down list.

For further details on how to upgrade to any of the remediating versions from your current installation, please refer to the JFrog Artifactory Upgrade Guide.

Acknowledgements

This issue was discovered and reported by Matthias Kaiser of Apple Information Security.

CVE-2024-3505 - Proxy Configuration Accessible to Low-privilege Users

CVE ID	Severity	CWE / Weakness Type	Date Published	Date Updated
CVE-2024-350	Medium	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	11 Apr 24	11 Apr 24

Description

JFrog Artifactory Self-Hosted versions prior to 7.77.3 are vulnerable to sensitive information disclosure whereby a low-privileged authenticated user can read the proxy configuration. This does not affect JFrog cloud deployments.

Severity

Medium

Affected Products

Product	Affected Version	Patched Version
Artifactory Self-Hosted	< 7.77.3	7.77.3

How to Fix

- **Cloud environments**: Cloud environments are not affected by this issue.
- **Self-Hosted environments**: To fix this issue, take the following action. Upgrade your version of Artifactory to one of the versions listed below.

Product	Version	Links
Artifactory (7.x)	7.77.3 or later (Self-Hosted)	• https://releases.jfrog.io/ • JFrog 7.77.3 Self-Hosted Release Information

Workarounds and Mitigations

None

Acknowledgements

This issue was discovered and reported by a JFrog customer.

CVE-2024-2247: JFrog Artifactory Cross-Site Scripting

CVE ID	Severity	Date Published	Date Updated
CVE-2024-2247	High	13 Mar 24	13 Mar 24

Description

JFrog Artifactory prior to version 7.77.7, is vulnerable to DOM-based cross-site scripting due to improper handling of the import override mechanism.

Severity

High

Affected Products

Product	Affected Version	Patched Version
Artifactory Self-Hosted	< = 7.77.6	7.77.7

How to Fix

- **Cloud Environments**: JFrog cloud environments are protected. No action is required for cloud instances.
- **Self Hosted Environments**: Update to version 7.77.7

Workarounds and Mitigations

Customers can block the import of the vulnerable script by the browser, using a WAF / reverse proxy rule that blocks requests to the following HTTP path: /ui/externals/import-map-overrides/dist/import-map-overrides.js

Weakness Type

CWE-79: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Acknowledgements

Reported by CaTz.

We are here for your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2023-42661: JFrog Artifactory Improper Input Validation Leads to Arbitrary File Write

CVE ID	Severity	Date Published	Date Updated
CVE-2023-42661	High	7 Mar 24	7 Mar 24

Description

JFrog Artifactory prior to version 7.76.2 is vulnerable to Arbitrary File Write of untrusted data, which may lead to DoS or Remote Code Execution when a specially crafted series of requests is sent by an authenticated user. This is due to insufficient validation of artifacts.

Severity

High

CVSSv3.1 Base Score: 7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Affected Products

Product	Affected Version	Patched Version
Artifactory (7.x)	Earlier than 7.76.2	7.76.2 or later (SaaS) 7.77.3 or later (On-prem)

Required Configuration for Exposure

This vulnerability affects all JFrog Artifactory deployments.

How to Fix

Cloud Environments: Affected Cloud environments have already been updated with a fixed version. No action is required for cloud instances.

Self Hosted Environments: To fix this issue, take the following action. Upgrade your version of Artifactory to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.77.3 or later (On-prem)	• https://releases.jfrog.io • Legacy PDF archive

Workarounds and Mitigations

No workarounds

Weakness Type

CWE-20: Improper Input validation

Acknowledgements

This issue was discovered and reported by Matthias Kaiser from Apple Information Security.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2023-42509: JFrog Artifactory Sensitive Data Leakage in Repository Configuration Process

CVE ID	Severity	Date Published	Date Updated
CVE-2023-42509	Medium	7 Mar 24	7 Mar 24

Description

JFrog Artifactory later than version 7.17.4 but prior to version 7.77.0 is vulnerable to an issue whereby a sequence of improperly handled exceptions in repository configuration initialization steps may lead to exposure of sensitive data.

Severity

Medium

CVSSv3.1 Base Score: 6.6 AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	7.17.4 and later but prior to version 7.77.0	• 7.77.0 and higher (SaaS) • 7.77.3 and higher (On-prem)

Required Configurations for Exposure

This vulnerability affects all JFrog Artifactory deployments.

How to Fix

Cloud Environments: Affected Cloud environments have already been upgraded with a fixed version. No action is required for cloud instances.

Self Hosted Environments: To fix this issue, the following action is required.

Upgrade your version of Artifactory to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.77.3 or newer (On-Prem)	• https://releases.jfrog.io • Legacy PDF archive

Workarounds and Mitigations

No workarounds

Weakness Type

CWE-755: Improper Handling of Exceptional Conditions

Acknowledgements

This issue was discovered and reported by Matthias Kaiser from Apple Information Security.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2023-42662: Improper SSO Mechanism may lead to Exposure of Access Tokens

CVE ID	Severity	Date Published	Date Updated
CVE-2023-42662	CRITICAL	6 Mar 24	6 Mar 24

Description

JFrog Artifactory versions 7.59 and above, but below 7.59.18, 7.63.18, 7.68.19, 7.71.8 are vulnerable to an issue whereby user interaction with specially crafted URLs could lead to exposure of user access tokens due to improper handling of the CLI / IDE browser based SSO integration.

Severity

CRITICAL

Affected Products

Product	Affected Versions	Patched Versions
Artifactory	• 7.59.17 and lower • 7.63.17 and lower • 7.69.18 and lower • 7.71.7 and lower	• 7.59.18 and higher • 7.63.18 and higher • 7.69.19 and higher • 7.71.8 and higher

How to Fix

Cloud Environments: Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self Hosted Environments: Update to one of a fixed version

Workarounds and Mitigations

Block access to the CLI token exchange API endpoint:
https://Artifactory-Host/access/api/v2/authentication/jfrog_client_login/token/*

Weakness Type

CWE-287: CWE-287 Improper Authentication

Acknowledgements

N/A

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2023-42508: JFrog Artifactory Improper Header Input Validation

CVE ID	Severity	Date Published	Date Updated
CVE-2023-42508	MEDIUM	10/04/2023	10/04/2023

Description

JFrog Artifactory prior to version 7.66.0 is vulnerable to specific endpoint abuse with a specially crafted payload, which can lead to unauthenticated users being able to send emails with manipulated email body.

Severity: Medium

CVSSv3.1 Base Score: 6.5 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.66.0	7.66.0 (SaaS) 7.68.7 (On-prem)

Required Configuration for Exposure

This vulnerability affects all JFrog Artifactory deployments.

How to Fix

How to fix depends upon your environment, as follows:

- Cloud Environments
- Self Hosted Environments

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.68.7	• https://releases.jfrog.io • Legacy PDF archive

Workarounds and Mitigations

No workarounds.

Weakness Type

CWE-20: Improper Input Validation.

Acknowledgements

This issue was discovered and reported by Iddo Eldor from Blindspot Security.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2022-0668: Artifactory Authentication Bypass

CVE ID	Severity	Date Published	Date Updated
CVE-2022-0668	MEDIUM	02/01/2023	02/01/2023

Description

JFrog Artifactory prior to 7.37.13 is vulnerable to Authentication Bypass, which can lead to Privilege Escalation when a specially crafted request is sent by an unauthenticated user.

Severity: Medium

CVSSv3 Score: 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.37.13	7.37.13
Artifactory (6.x)	< 6.23.41	Latest version of 6.23.x

Required Configuration for Exposure

This vulnerability affects all JFrog Artifactory deployments.

How to Fix

Cloud Enviornments: Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.37.13	https://releases.jfrog.io

Exploitation Status

JFrog is not aware of publicly available exploits and malicious exploitation attempts.

Weakness Type

CWE-274: Improper Handling of Insufficient Privileges.

Acknowledgements

This issue was discovered and reported by Matthias Kaiser and Jonni Passki of Apple Information Security.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-45721: Cross-Site Script (XSS) on User REST API

CVE ID	Severity	Date Published	Date Updated
CVE-2021-45721	MEDIUM	07/05/202	07/05/2022

Description

JFrog Artifactory prior to version 7.29.8 and 6.23.38is vulnerable to Reflected Cross-Site Scripting (XSS) through one of the XHR parameters in Users REST API endpoint.

Severity: Medium

CVSSv3.1 Score: 6.1AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.29.8	7.29.8
Artifactory (6.x)	< 6.23.38	6.23.38

Required Configuration

This vulnerability affects JFrog Artifactory deployments.

This issue requires an attacker to have authenticated access to JFrog Artifactory as Administrator

How to Fix

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.29.8 and above	https://releases.jfrog.io
Artifactory (6.x)	6.23.38 and above	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE- 79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Acknowledgements

This issue was discovered and reported by Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-46687: Sensitive data exposure on proxy endpoint for Project Admin

CVE ID	Severity	Date Published	Date Updated
CVE-2021-46687	MEDIUM	07/05/2022	07/05/2022

Description

JFrog Artifactory prior to version 7.31.10 and 6.23.38 is vulnerable to Sensitive Data Exposure through the Project Administrator REST API.

Severity: Medium

CVSSv3.1 Score: 4.9AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.31.10	7.31.10
Artifactory (6.x)	< 6.23.38	6.23.38

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This issue requires an attacker to have authenticated access to JFrog Artifactory as Project Administrator.

How to Fix

Cloud Enviornments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.31.10 and above	https://releases.jfrog.io
Artifactory (6.x)	6.23.38 and above	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE- 359: Exposure of Private Personal Information to an Unauthorized Actor

Acknowledgements

This issue was discovered and reported by Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-23163: Cross-Site Request Forgery on REST using Basic Auth

CVE ID	Severity	Date Published	Date Updated
CVE-2021-23163	LOW	07/05/2022	07/05/2022

Description

JFrog Artifactory prior to version 7.33.6 and 6.23.38, is vulnerable to CSRF (Cross-Site Request Forgery) for specific endpoints.

Severity: LOW

CVSSv3.1 Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.33.6	7.33.6
Artifactory (6.x)	< 6.23.38	6.23.38

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This issue requires a user to enter their credentials in a www-authenticate negotiation, or have accessed some of the Artifactory REST APIs using basic credentials in the URL. (user:pass@artifactory-domain).

How to Fix

Cloud

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.33.6 and above	https://releases.jfrog.io
Artifactory (6.x)	6.23.38 and above	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE-352: Cross-Site Request Forgery (CSRF)

Acknowledgements

This issue was discovered and reported by Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-41834: Artifactory Broken Access Control on Copy Artifact

CVE ID	Severity	Date Published	Date Updated
CVE-2021-41834	MEDIUM	18/5/2022	18/5/2022

Description

JFrog Artifactory prior to version 7.28.0 and 6.23.38, is vulnerable to Broken Access Control, the copy functionality can be used by a low-privileged user to read and copy any artifact that exists in the Artifactory deployment due to improper permissions validation.

Severity: Medium CVSSv3 Score: 5.3 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.28.0	7.28.0
Artifactory (6.x)	< 6.23.38	6.23.38

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This vulnerability requires authenticated access to JFrog Artifactory and knowing a path of a repository or artifact that the user does not have access to.

How to Fix

Cloud

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.28.0	https://releases.jfrog.io
Artifactory (6.x)	6.23.38	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE-284: Improper Access Control

Acknowledgements

Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-45730: Artifactory Broken Access Control on Repository Layouts Configuration

CVE ID	Severity	Date Published	Date Updated
CVE-2021-45730	MEDIUM	18/5/2022	18/5/2022

Description

JFrog Artifactory prior to 7.31.10, is vulnerable to Broken Access Control where a Project Admin is able to create, edit and delete Repository Layouts while Repository Layouts configuration should only be available for Platform Administrators.

Severity: MEDIUM

CVSSv3.1 Base Score:6.0CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.31.10	7.31.10

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This vulnerability requires authenticated access to JFrog Artifactory and Project Admin permissions.

How to Fix

Cloud

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your Artifactory version to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.31.10	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE-284: Improper Access Control

Acknowledgements

Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-46270: Artifactory Project Admin Repository Name Disclosure

CVE ID	Severity	Date Published	Date Updated
CVE-2021-46270	LOW	03/02/2022	03/02/2022

Description

JFrog Artifactory prior to 7.31.10, is vulnerable to Broken Access Control where a Project Admin user is able to list all available repository names due to insufficient permission validation.

Severity: LOW

CVSSv3.1 Base Score:2.7AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.31.10	7.31.10

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This issue requires authenticated access to JFrog Artifactory and Project Admin permissions.

How to Fix

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your Artifactory version to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.31.10	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE-284: Improper Access Control

Acknowledgements

Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-45074: Artifactory Broken Access Control on Delete OAuth Tokens

CVE ID	Severity	Date Published	Date Updated
CVE-2021-45074	MEDIUM	03/02/2022	03/02/2022

Description

JFrog Artifactory prior to 7.29.3 and 6.23.38, is vulnerable to Broken Access Control, a low-privileged user is able to delete other known usersOAuthtoken, which will force re-authentication on an active session or in the next UI session.

Severity: MEDIUM

CVSSv3.1 Base Score:4.3AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.29.3	7.29.3
Artifactory (6.x)	< 6.23.38	6.23.38

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This vulnerability requires authenticated access to JFrog Artifactory and guessing the username of another user, as well as an OAuth token.

How to Fix

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your Artifactory version to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	7.29.3	https://releases.jfrog.io
Artifactory (6.x)	6.23.38	https://releases.jfrog.io

Workarounds and Mitigations

There aren't any suggested workarounds to this issue besides upgrading to a fixed version.

Weakness Type

CWE-284: Improper Access Control

Acknowledgements

Maxime Escourbiac and Maxence Schmitt at Michelin CERT.

We Are Here For Your Questions (JFrog Support Team)**

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2021-3860: Artifactory Low Privileged Blind SQL Injection

CVE ID	Severity	Date Published	Date Updated
CVE-2021-3860	HIGH	12/15/2021	12/15/2021

Description

JFrog Artifactory prior to 7.25.4 (Enterprise+ subscriptions only), is vulnerable to Blind SQL Injection by a low privileged authenticated user due to incomplete validation when performing an SQL query.

Severity: High

CVSSv3 Score: 8.8 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.25.4	7.24.7, 7.23.8, 7.21.14, 7.19.12, 7.18.11, 7.17.14, 7.12.10, 7.11.8
Artifactory (6.x)	< 6.23.30	Latest version of 6.23.x

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory and JFrog edge deployments with Enterprise+ subscriptions only.

This issue requires an attacker to have authenticated access to JFrog Artifactory.

> **Note**
>
> If your environment permits anonymous access, there is a higher potential of exposure to the vulnerability.

How to Fix

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your version of Artifactory or Edge to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	Latest	https://releases.jfrog.io
Artifactory (7.x)	7.24.7	https://releases.jfrog.io
Artifactory (7.x)	7.23.8	https://releases.jfrog.io
Artifactory (7.x)	7.21.14	https://releases.jfrog.io
Artifactory (7.x)	7.19.12	https://releases.jfrog.io
Artifactory (7.x)	7.18.11	https://releases.jfrog.io
Artifactory (7.x)	7.17.14	https://releases.jfrog.io
Artifactory (7.x)	7.12.10	https://releases.jfrog.io
Artifactory (7.x)	7.11.8	https://releases.jfrog.io
Artifactory (6.x)	Latest 6.23.x version	https://releases.jfrog.io

Workarounds and Mitigations

You can mitigate the impact of this issue by following best practices and disabling anonymous access to the JFrog Platform. Please review the best practices for disabling anonymous access in the JFrog knowledge base.

Note

Anonymous Access is disabled by default for new Artifactory and Edge installations starting from versions 6.12.0 and 7.0.0.

Exploitation Status

JFrog is not aware of publicly available exploits and malicious exploitation attempts.

Weakness Type

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Acknowledgements

This issue was discovered and reported by a JFrog customer.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

CVE-2022-0573: Artifactory Vulnerable to Deserialization of Untrusted Data

CVE ID	Severity	Date Published	Date Updated
CVE-2022-0573	HIGH	12/5/2022	

Description

JFrog Artifactory prior to 7.36.1 and 6.23.41, is vulnerable to Insecure Deserialization of untrusted data which can lead to DoS, Privilege Escalation and Remote Code Execution when a specially crafted request is sent by a low privileged authenticated user due to insufficient validation of a user-provided serialized object.

Severity: HIGH

CVSSv3.1 Base Score:8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Products

Product	Affected Versions	Patched Versions
Artifactory (7.x)	< 7.36.1	• 7.17.16 • 7.18.12 • 7.19.13 • 7.21.25 • 7.25.9 • 7.27.15 • 7.29.10 • 7.31.16 • 7.33.12 • 7.34.4 • 7.35.1 • 7.36.1
Artifactory (6.x)	< 6.23.41	6.23.41

Required Configuration for Exposure

This vulnerability affects JFrog Artifactory deployments.

This issue requires an attacker to have authenticated access to JFrog Artifactory.

If your environment permits anonymous access, there is a higher potential of exposure to the vulnerability.

How to Fix

Cloud Environments

Affected Cloud environments have already been fortified with a fixed version. No action is required for cloud instances.

Self-Hosted Environments

To fix this issue, there is required action.

Upgrade your Artifactory version to one of the versions listed below:

Product	Version	Link
Artifactory (7.x)	latest	https://releases.jfrog.io
Artifactory (7.x)	7.17.16	https://releases.jfrog.io
Artifactory (7.x)	7.18.12	https://releases.jfrog.io
Artifactory (7.x)	7.19.13	https://releases.jfrog.io
Artifactory (7.x)	7.21.25	https://releases.jfrog.io
Artifactory (7.x)	7.25.9	https://releases.jfrog.io
Artifactory (7.x)	7.27.15	https://releases.jfrog.io
Artifactory (7.x)	7.29.10	https://releases.jfrog.io
Artifactory (7.x)	7.31.16	https://releases.jfrog.io
Artifactory (7.x)	7.33.12	https://releases.jfrog.io
Artifactory (7.x)	7.34.3	https://releases.jfrog.io
Artifactory (7.x)	7.35.1	https://releases.jfrog.io
Artifactory (7.x)	7.36.1	https://releases.jfrog.io
Artifactory (6.x)	Latest 6.23.x version	https://releases.jfrog.io

Workarounds and Mitigations

You can mitigate the impact of this issue by following best practices and disabling anonymous access to the JFrog Platform. Please review the best practices for disabling anonymous access in the JFrog Knowledge Base.

Note

Anonymous Access is disabled by default for new Artifactory and Edge installations starting from versions 6.12.0 and 7.0.0.

Weakness Type

CWE-502: Deserialization of Untrusted Data

Acknowledgements

This issue was discovered and reported by Matthias Kaiser and Jonni Passki of Apple Information Security.

We Are Here For Your Questions (JFrog Support Team)

If you have questions or concerns regarding this advisory, please raise a support request at JFrog support portal.

Updated about 2 months ago

← JFrog Grid Release Information

Deprecations →

Did this page help you?

Yes No

Products

Artifactory
Distribution
Xray
Advanced Security
Runtime
AppTrust
Curation
ML
AI Catalog

Resources

Events
Integrations
Software Supply Chain Topics
Open Source
JFrog Trust
Compare JFrog
JFrog Academy

Company

About
Management
Investor Relations
Partners
Customers

Developer

Community
Downloads
Community Events
Community Forum

Careers

Press

Contact Us

Brand Guidelines

Follow Us

© 2026 JFrog Ltd All Rights Reserved

© 2026 JFrog Ltd All Rights Reserved

Terms of Use Privacy Policy Cookies Settings Cookies Policy