Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0272

Kwetsbaarheden verholpen in JFrog Artifactory

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 31-07-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

JFrog heeft meerdere kwetsbaarheden verholpen in JFrog Artifactory

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van JFrog Artifactory.

- Er is een privilege-escalatie mogelijk doordat het systeem de scope van tokens niet controleert, waardoor een aanvaller zijn rechten kan verhogen.
- Daarnaast kunnen gebruikers met beperkte rechten toegang krijgen tot geprivilegieerde autorisatiematerialen en kunnen zij via een zwakke refresh token validatie een administrator token verkrijgen.
- Verder is er een deserialisatieprobleem in de package handling, wat kan leiden tot ongeautoriseerde code-uitvoering of datamanipulatie.
- Onjuiste URL-validatie maakt het mogelijk om ongeautoriseerde verzoeken te maken en interne services of gecachte data te benaderen.
- Een path traversal kwetsbaarheid kan leiden tot het schrijven van bestanden buiten de bedoelde directory.
- Er is ook een autorisatiezwakte in de metadata handling, waardoor gebruikers met beperkte rechten metadata kunnen wijzigen.
- Specifieke componenten zoals de Ansible repository, Terraform remote repositories en Cargo remote repository zijn kwetsbaar voor Server-Side Request Forgery (SSRF) aanvallen, waarbij ongewenste HTTP-verzoeken kunnen worden uitgevoerd en de reacties daarvan kunnen worden ingezien.
- Verder is er een kwetsbaarheid in het interne authenticatiesysteem die privilege-escalatie mogelijk maakt.
- Ten slotte kunnen gebruikers met leesrechten op een repository ook omgevingsvariabelen van andere repositories inzien, wat kan leiden tot blootstelling van vertrouwelijke build secrets.

OpenAI heeft in een publieke blog-post vermeld dat hierboven beschreven kwetsbaarheden als ZeroDay kwetsbaarheid zijn misbruikt door een OpenAI model om zelfstandig toegang te krijgen tot het internet en daarmee in staat te zijn geweest een derde partij aan te vallen. OpenAI heeft JFrog onmiddellijk in kennis gesteld zodat JFrog de kwetsbaarheden zo spoedig mogelijk kon verhelpen.

Oplossingen

JFrog heeft updates uitgebracht om de kwetsbaarheden in JFrog Artifactory te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases
- https://docs.jfrog.com/releases/docs/jfrog-security-advisories
- https://openai.com/index/hugging-face-model-evaluation-security-incident/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-42016	8.1 HIGH
CVE-2026-42017	8.8 HIGH
CVE-2026-65616	8.8 HIGH
CVE-2026-65617	8.8 HIGH
CVE-2026-65618	6.5 MEDIUM
CVE-2026-65921	8.8 HIGH
CVE-2026-65922	7.1 HIGH
CVE-2026-65923	6.8 MEDIUM
CVE-2026-65924	6.5 MEDIUM
CVE-2026-65925	6.5 MEDIUM
CVE-2026-66014	8.8 HIGH
CVE-2026-66015	7.2 HIGH
CVE-2026-66018	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management
CWE-287	Improper Authentication
CWE-347	Improper Verification of Cryptographic Signature
CWE-502	Deserialization of Untrusted Data
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

JFrog
Artifactory

Disclaimer