BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-45
Fecha de publicación: 3/10/2024
Tema: Vulnerabilidades Criticas en Jenkins
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Jenkins weekly: 2.479
- Jenkins LTS: 2.462.3
- Credentials Plugin: 1381.v2c3a_12074da_b_
- OpenID Connect Authentication Plugin: 4.355.v3a_fb_fca_b_96d4

Descripción

Se ha reportado vulnerabilidades criticas en Jenkins, entre ellas se pueden destacar: **CVE-2024-47803, CVE-2024-47804, CVE-2024-47805, CVE-2024-47806 y CVE-2024-47807**, estas ultimas dos vulnerabilidades, con criticidad alta y score CVSSv3 8.1, con las demás aún no se ha definido el score. Estas fallas podrían permitir a los atacantes robar datos confidenciales, eludir las restricciones de seguridad e incluso obtener el control total de los servidores de Jenkins.

Las vulnerabilidades más graves incluyen:

- **CVE-2024-47803:** Esta vulnerabilidad expone secrets de varias líneas, como claves API y contraseñas, a través de mensajes de error. Se podría acceder a esta información a través de logs del sistema, lo que podría dar a los atacantes acceso a credenciales confidenciales.

- **CVE-2024-47804:** Los atacantes pueden explotar esta falla para eludir las restricciones de creación de elementos, lo que les permite crear elementos temporales y, con más permisos, persistir estos elementos para obtener acceso no autorizado.

- **CVE-2024-47805:** Esta vulnerabilidad permite a los usuarios con permisos de “Lectura extendida” (Extended Read) ver los valores de credenciales cifradas, lo que potencialmente expone información confidencial como certificados y archivos secretos.

- **CVE-2024-47806 y CVE-2024-47807:** estas vulnerabilidades estan presenten el plugin de autenticación de OpenID Connect, el cual no pueden validar los reclamos/pedidos cruciales de los ID Tokens. Este vulnerabilidad podría permitir a los atacantes eludir la autenticación y, potencialmente, obtener acceso de administrador al servidor Jenkins.

El equipo de Jenkins recomienda tomar acciones correctivas los mas pronto posibles aplicando los parches de seguridad proveidos.

Solución

El equipo de Jenkins ha publicado parches de seguridad para corregir dichas vulnerabilidades, puede dirigirse a los siguientes enlances para tener mas información:

- https://www.jenkins.io/changelog-stable/
- https://www.jenkins.io/security/advisory/2024-10-02/#jenkins-security-advisory-2024-10-02

A continuación se listan las versiones de los productos afectados con los parches de seguridad que corrigen las vulnerabilidades mencionadas:

- **Jenkins weekly** debe ser actualizado a la version 2.479
- **Jenkins LTS** debe ser actualizado a la version 2.462.3
- **Credentials Plugin** debe ser actualizado a la version 1381.v2c3a_12074da_b_
- **OpenId Connect Authentication Plugin** debe ser actualizado a la version 4.355.v3a_fb_fca_b_96d4

Información adicional:

- https://www.jenkins.io/security/advisory/2024-10-02/#jenkins-security-advisory-2024-10-02
- https://www.jenkins.io/changelog-stable/
- https://securityonline.info/security-vulnerabilities-uncovered-in-jenkins-immediate-updates-recommended/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com