BEACON LAB
C S I R T

CYBOLT
Security Innovation

# Boletín de Alerta

Boletín Nro.: 2024-26
Fecha de publicación: 05/09/2024
Tema: Vulnerabilidades criticas en producto Cisco Smart Licensing Utility
Traffic Light Protocol (TLP): White


## Producto(s) afectado:

- Cisco ISE 3.2 (3.2P7 - septiembre de 2024)
- Cisco ISE 3.3 (3.3P4 - octubre de 2024)
- Smart licensing Utiliy <= 2.2.0

## Descripción

El equipo de Cisco ha publicado actualizaciones de seguridad para dos fallas de seguridad críticas que afectan a su producto Smart Licensing Utility y que podrían permitir a atacantes remotos no autenticados elevar sus privilegios o acceder a información confidencial.

A continuación se describen ambas vulnerabilidad criticas:

- CVE-2024-20439 (puntuación CVSS: 9,8): la presencia de una credencial de usuario estática no documentada para una cuenta administrativa que un atacante podría explotar para iniciar sesión en un sistema afectado.

- CVE-2024-20440 (puntuación CVSS: 9,8): una vulnerabilidad que surge debido a un archivo de registro de depuración excesivamente detallado que un atacante podría explotar para acceder a dichos archivos mediante una solicitud HTTP diseñada y obtener credenciales que se pueden usar para acceder a la API.

Cisco reporta que ambas vulnerabilidades no dependen unas de otras para ser explotadas y confirman que "no son explotables a menos que un usuario haya iniciado Cisco Smart Licensing Utility y esté ejecutándose activamente".

| Cisco Smart License Utility Release | Primer Version Arreglada |
|---|---|
| 2.0.0 | Migrar a una version Segura. |
| 2.1.0 | Migrar a una version Segura. |
| 2.2.0 | Migrar a una version Segura. |

| Cisco Smart License Utility Release | Primer Version Arreglada |
|---|---|
| 2.3.0 | No es vulnerable. |

## Solución

El proveedor estarán publicando los parches de seguridad de acuerdo a su plan de actualizaciones:

https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

Puede encontrar las versiones seguras en el siguiente enlace o contacte con su proveedor local:

https://www.cisco.com/c/en/us/support/index.html

## Información adicional:

- https://thehackernews.com/2024/09/cisco-fixes-two-critical-flaws-in-smart.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
- https://www.tenable.com/cve/CVE-2024-20439

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com