Cisco ha publicado actualizaciones de seguridad para dos vulnerabilidades críticas en su Smart Licensing Utility, que podrían permitir a atacantes remotos no autenticados aumentar sus privilegios o acceder a información sensible.

A continuación, un resumen de las dos vulnerabilidades:

- CVE-2024-20439 (puntuación CVSS: 9.8): Se refiere a la existencia de una credencial de usuario estática no documentada para una cuenta administrativa. Un atacante podría aprovechar esta vulnerabilidad para iniciar sesión en un sistema afectado.
- CVE-2024-20440 (puntuación CVSS: 9.8): Esta falla surge de un archivo de registro de depuración demasiado detallado, que un atacante podría explotar mediante una solicitud HTTP especialmente diseñada para acceder a estos archivos y obtener credenciales para utilizar la API.

Aunque estas vulnerabilidades pueden ser explotadas de forma independiente, Cisco aclara en su informe que «no son explotables a menos que el Cisco Smart Licensing Utility haya sido iniciado y esté en ejecución por un usuario».

Estas vulnerabilidades, detectadas durante pruebas de seguridad internas, no afectan a los productos Smart Software Manager On-Prem ni Smart Software Manager Satellite.

Se recomienda a los usuarios que utilicen las versiones 2.0.0, 2.1.0 y 2.2.0 de Cisco Smart License Utility que actualicen a una versión corregida. La versión 2.3.0 no está afectada por estos fallos.

Por otra parte, Cisco también ha corregido una vulnerabilidad de inyección de comandos en su Identity Services Engine (ISE), que podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el sistema operativo subyacente y eleve sus privilegios a nivel de root.

La vulnerabilidad, identificada como CVE-2024-20469 (puntuación CVSS: 6.0), requiere que el atacante posea privilegios de administrador válidos en el dispositivo afectado.

> *«Este fallo se debe a una validación inadecuada de los datos proporcionados por el usuario. Un atacante podría explotarlo enviando un comando CLI malicioso. Si se explota con éxito, permitiría al atacante elevar privilegios a root»,* explicó la empresa.

Las versiones afectadas son las siguientes:

- Cisco ISE 3.2 (3.2P7 – Sep 2024)
- Cisco ISE 3.3 (3.3P4 – Oct 2024)

La empresa ha informado que existe un código de prueba de concepto (PoC) disponible, aunque no se tiene conocimiento de un uso malintencionado de esta vulnerabilidad.