Dos vulnerabilidades de seguridad recientemente corregidas en Cisco Smart Licensing Utility están siendo activamente explotadas, según el SANS Internet Storm Center.

Las dos fallas críticas son:

- CVE-2024-20439 (Puntuación CVSS: 9.8): Unas credenciales estáticas no documentadas para una cuenta administrativa, lo que permitiría a un atacante acceder al sistema afectado.
- CVE-2024-20440 (Puntuación CVSS: 9.8): Un archivo de registro de depuración que contiene información excesiva, permitiendo que un atacante, mediante una solicitud HTTP manipulada, acceda a credenciales para la API.

Si se explotan con éxito, estas vulnerabilidades pueden permitir que un atacante obtenga acceso administrativo y extraiga archivos de registro con información confidencial, incluidas credenciales.

No obstante, estas fallas solo pueden ser explotadas si la utilidad está en ejecución.

Las versiones afectadas incluyen 2.0.0, 2.1.0 y 2.2.0, pero Cisco ya corrigió los problemas en septiembre de 2024. La versión 2.3.0 no es vulnerable.

En marzo de 2025, investigadores han detectado intentos de explotación activa de estas vulnerabilidades, según Johannes B. Ullrich, investigador del SANS Technology Institute. Además, los atacantes también están aprovechando otras fallas, como un posible problema de filtración de información (CVE-2024-0305, CVSS: 5.3) en Guangzhou Yingke Electronic Technology Ncast.

Se desconoce quién está detrás de estos ataques o cuál es su objetivo final. Ante estos intentos de explotación, es fundamental que los usuarios apliquen las actualizaciones de seguridad correspondientes para una protección óptima.