La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) ha informado que actores malintencionados están explotando la función heredada Cisco Smart Install (SMI) para acceder a datos confidenciales.

La agencia indicó que ha observado cómo los atacantes *«adquieren archivos de configuración del sistema utilizando protocolos o software disponibles en los dispositivos, como abusando de la función heredada Cisco Smart Install».*

CISA también destacó que sigue detectando el uso de contraseñas débiles en dispositivos de red Cisco, lo que los deja vulnerables a ataques de descifrado de contraseñas. Los tipos de contraseñas se refieren a los algoritmos utilizados para proteger las contraseñas de los dispositivos Cisco dentro de los archivos de configuración del sistema.

Si los atacantes logran acceder a un dispositivo de esta manera, podrían obtener fácilmente los archivos de configuración del sistema, lo que podría llevar a una mayor compromisión de las redes de la víctima.

> *«Las organizaciones deben garantizar que todas las contraseñas en los dispositivos de red estén protegidas con un nivel adecuado de seguridad»,* afirmó CISA, recomendando *«la protección de contraseñas de tipo 8 para todos los dispositivos Cisco, a fin de proteger las contraseñas en los archivos de configuración».*

CISA también insta a las empresas a revisar la advertencia de la Agencia de Seguridad Nacional (NSA) sobre el uso indebido del protocolo Smart Install y la Guía de Seguridad de Infraestructura de Red para obtener recomendaciones de configuración.

Otras prácticas recomendadas incluyen el uso de un algoritmo de hashing robusto para almacenar contraseñas, evitar la reutilización de contraseñas, asignar contraseñas fuertes y complejas, y evitar el uso de cuentas grupales que no ofrezcan responsabilidad individual.

Este informe coincide con la advertencia de Cisco sobre la disponibilidad pública de un

código de prueba de concepto (PoC) para la vulnerabilidad CVE-2024-20419 (puntuación CVSS: 10.0), un fallo crítico en Smart Software Manager On-Prem (Cisco SSM On-Prem) que podría permitir a un atacante remoto y no autenticado cambiar la contraseña de cualquier usuario.

El gigante de los equipos de red también ha alertado sobre varias vulnerabilidades críticas (CVE-2024-20450, CVE-2024-20452 y CVE-2024-20454, puntuaciones CVSS: 9.8) en los teléfonos IP de las Series Small Business SPA300 y SPA500, que podrían permitir a un atacante ejecutar comandos arbitrarios en el sistema operativo subyacente o provocar una condición de denegación de servicio (DoS).

> *«Estas vulnerabilidades existen porque los paquetes HTTP entrantes no se verifican correctamente en busca de errores, lo que podría dar lugar a un desbordamiento de búfer»*, explicó Cisco en un boletín publicado el 7 de agosto de 2024.
>
> *«Un atacante podría explotar esta vulnerabilidad enviando una solicitud HTTP especialmente diseñada a un dispositivo afectado. Un exploit exitoso podría permitir al atacante desbordar un búfer interno y ejecutar comandos arbitrarios con privilegios de root».*

La compañía también mencionó que no tiene planes de lanzar actualizaciones de software para corregir estas vulnerabilidades, ya que los dispositivos han alcanzado su estado de fin de vida útil (EoL), lo que obliga a los usuarios a actualizar a modelos más recientes.