Cisco ha emitido una advertencia acerca de una reciente vulnerabilidad zero-day en el sistema operativo IOS XE, que ha sido activamente aprovechada por un actor de amenazas desconocido para implementar un programa malicioso basado en Lua en dispositivos vulnerables.

Esta vulnerabilidad se ha catalogado con el nombre CVE-2023-20273 (con una puntuación CVSS de 7.2). La vulnerabilidad está relacionada con un fallo de escalada de privilegios en la característica de la interfaz web y se ha utilizado en conjunto con la vulnerabilidad CVE-2023-20198 como parte de una cadena de explotación.

> Según Cisco, *«el atacante primero aprovechó la vulnerabilidad CVE-2023-20198 para obtener acceso inicial y emitió un comando de nivel de privilegio 15 para crear un usuario y una combinación de contraseña locales. Esto permitió al usuario iniciar sesión con acceso de usuario normal.»*

Luego, el atacante aprovechó otro componente de la característica de la interfaz web, utilizando el nuevo usuario local para elevar los privilegios al nivel de «root» y escribir el programa malicioso en el sistema de archivos, lo cual se ha denominado como CVE-2023-20273.

Un portavoz de Cisco informó que se ha identificado una solución que abarca ambas vulnerabilidades y estará disponible para los clientes a partir del 22 de octubre de 2023. Mientras tanto, se recomienda desactivar la función del servidor HTTP.

A pesar de que Cisco había mencionado previamente que una vulnerabilidad de seguridad en el mismo software, que ahora está parchada, había sido aprovechada para instalar una puerta trasera, la empresa ha evaluado que esta vulnerabilidad ya no está relacionada con la actividad maliciosa, debido al descubrimiento de esta nueva vulnerabilidad zero-day.

> La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA)

> advierte que *«un actor remoto no autenticado podría aprovechar estas vulnerabilidades para tomar el control de un sistema afectado. Estas vulnerabilidades, en concreto, permiten al actor crear una cuenta privilegiada que proporciona un control total sobre el dispositivo.»*

La explotación exitosa de estas vulnerabilidades podría permitir a los atacantes obtener acceso remoto ilimitado a enrutadores y conmutadores, monitorear el tráfico de la red, inyectar y redirigir el tráfico de la red, y utilizar estos dispositivos como un punto de apoyo persistente en la red, debido a la falta de soluciones de protección para estos dispositivos.

Este desarrollo surge en un momento en que se estima que más de 41,000 dispositivos Cisco que ejecutan el software IOS XE vulnerable han sido comprometidos por actores de amenazas que aprovechan estas dos vulnerabilidades de seguridad, según datos de Censys y LeakIX.

> *«Al 19 de octubre, el número de dispositivos Cisco comprometidos ha disminuido a 36,541. Los principales objetivos de esta vulnerabilidad no son las grandes corporaciones, sino entidades más pequeñas e individuos»,* afirmó la firma de gestión de superficie de ataque.