El acceso encubierto que se insertó en dispositivos de Cisco al explotar un par de vulnerabilidades de día cero en el software IOS XE ha sido alterado por el actor malicioso con el propósito de evitar su detección mediante métodos de identificación previamente utilizados.

> *«La inspección del tráfico de red en un dispositivo comprometido ha demostrado que el actor malicioso ha mejorado el implante para llevar a cabo una comprobación adicional del encabezado. Por lo tanto, en muchos dispositivos, el implante aún está activo, pero ahora solo responde si se establece el encabezado de Autorización HTTP correcto»,* informó el equipo de Fox-IT de NCC Group.

Estos ataques implican la explotación de CVE-2023-20198 (puntuación CVSS: 10.0) y CVE-2023-20273 (puntuación CVSS: 7.2) en una serie de exploits que proporcionan al actor malicioso la capacidad de acceder a los dispositivos, crear una cuenta con privilegios y, en última instancia, implementar un implante basado en Lua en los dispositivos.

Este desarrollo se produce mientras Cisco ha comenzado a liberar actualizaciones de seguridad para abordar estos problemas, con más actualizaciones programadas para ser lanzadas en una fecha aún por determinar.

Actualmente, la identidad exacta del actor malicioso detrás de esta campaña no se conoce, aunque se estima que el número de dispositivos afectados se encuentra en el rango de miles, según datos compartidos por VulnCheck y la empresa de gestión de superficie de ataque Censys.

> *«Las infecciones parecen ser ataques masivos. Puede llegar el momento en que los atacantes revisen su botín y determinen si lo obtenido tiene algún valor»,* señaló Mark Ellzey, Investigador Senior de Seguridad en Censys

Sin embargo, en los últimos días, el número de dispositivos comprometidos ha experimentado una brusca caída, pasando de aproximadamente 40,000 a unos pocos cientos, lo que ha llevado a la especulación de que podría haber habido modificaciones internas para ocultar la presencia del implante.

Las últimas alteraciones en el implante, descubiertas por Fox-IT, explican esta repentina y drástica disminución, ya que más de 37,000 dispositivos todavía se han identificado como comprometidos con el implante.

Cisco, por su parte, ha confirmado el cambio de comportamiento en sus avisos actualizados y ha compartido un comando curl que puede ser ejecutado desde un lugar de trabajo para verificar la presencia del implante en los dispositivos:

```
curl -k -H "Authorization:
0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST
"https://systemip/webui/logoutconfirm.html?logon_hash=1"
```

Cisco aclara que si la solicitud devuelve una cadena hexadecimal, como «0123456789abcdef01», significa que el implante está presente.