ALERTA DE SEGURIDAD DE LA INFORMACIÓN
EXPLOTACIÓN DE VULNERABILIDAD EN CISCO IOS XE
TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública comparte la información dada a conocer por Cisco de la amenaza que supone la explotación activa de la vulnerabilidad CVE-2023-20198, que afecta a su software Cisco IOS XE. Este sistema operativo es fundamental en el funcionamiento de numerosos productos de la empresa, los que son usados por miles de organizaciones en el mundo, incluyendo a Chile.

La explotación de CVE-2023-20198 es considerada **de riesgo crítico**, como detallamos en nuestra respectiva alerta de vulnerabilidad publicada el 17 de octubre: https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00921-01/.

La empresa puso a disposición de sus clientes un parche para esta vulnerabilidad, el que también resuelve otra conocida como CVE-2023-20273. Esta actualización puede ser conseguida en el sitio respectivo del proveedor (https://software.cisco.com/download/home).

Cisco describe las características de estas vulnerabilidades aquí: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z.

Por medio del presente documento, queremos recalcar la importancia de implementar este parche de seguridad, y de, en tanto no esté aún implementada la actualización, realizar las medidas de mitigación delineadas a continuación.

Medidas de mitigación

Las medidas de mitigación publicadas por Cisco (https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/) deben ser puestas en práctica mientras los sistemas vulnerables puedan ser actualizados.

La compañía detalló lo siguiente (recomendamos guiarse directamente por lo indicado por Cisco y usar la siguiente traducción solo como referencia):

- Para ser vulnerable, su software Cisco IOS XE debe tener la función de UI web habilitada.
    - Para saber HTTP Server está habilitada, el administrador debe loguearse en el sistema y usar el comando **show running-config | include ip http server|secure|active** en el CLI para saber si los comandos **ip http server command** o **ip http secure-server** están presentes en la configuración global. Si uno o ambos comandos están presentes, el sistema es vulnerable.

- Si el comando **ip http server** está presente y la configuración también contiene **ip http active-session-modules none**, la vulnerabilidad no es explotable a través de HTTP.
- Si el comando **ip http secure-server** está presente y la configuración también contiene **ip http secure-active-session-modules none** la vulnerabilidad no es explotable a través de HTTPS.

- Como medida de mitigación mientras llega el parche, recomendamos:
  - Desactivar el componente web UI (HTTP Server) en sistemas expuestos a internet.
    - Para desactivar HTTP Server, se debe usar el comando `no ip http server` o `no ip http secure-server` en modo **global configuration**.
    - Si tanto HTTP server como HTTPS server están en uso, se requieren ambos comandos del punto anterior para desactivar la función HTTP Server.
  - Evitar exponer el web UI y servicios de administración a internet o a redes que no sean de confianza.
- **Estas medidas reducen el riesgo, pero no lo eliminan** por completo, pudiendo los atacantes ya haberse desplegado en los sistemas vulnerables.
- Cisco llama a buscar indicios de infección usando los indicadores de compromiso que han listado en https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/.
  - El implante se guarda bajo la ruta de archivo **/usr/binos/conf/nginx-conf/cisco_service.conf**, que contiene dos secuencias variables de caracteres hexadecimales. Este implante no es persistente, pero las cuentas de usuario local creadas por el atacante lo son.
  - Cisco llama asimismo a revisar la presencia de usuarios nuevos o no explicados en dispositivos que usen IOS XE.
    - Chequear los logs de sistema ante la presencia de mensajes de log donde el "user" sea "cisco_tac_admin", "cisco_support" o cualquier usuario local desconocido para el administrador de red:
      - **%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line**
      - **%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:42:13 UTC Wed Oct 11 2023**
    - El mensaje %SYS-5-CONFIG_P estará presente para cada instancia en que un usuario haya accedido a la web UI. Se debe revisar si aparecen usernames nuevos o desconocidos en ese mensaje.
    - Chequear los logs de sistema ante la presencia del siguiente mensaje en el que el filename sea un filename desconocido que no se correlaciona con una acción de instalación de archivo esperada:
      - **%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD filename**

IOC:
5.149.249[.]74
154.53.56[.]231

Usernames:
cisco_tac_admin
cisco_support

Les pedimos asimismo que se mantengan al tanto de nuestras alertas a través de los canales oficiales del CSIRT (https://www.csirt.gob.cl/noticias, https://twitter.com/CSIRTGOB).

Finalmente, les recordamos que ante cualquier inquietud sobre esta información u otros requerimientos para detectar y mitigar vulnerabilidades o reportar un incidente, pueden contactar al CSIRT de Gobierno a través del correo electrónico incidentes@interior.gob.cl o llamar al 1510.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.24 10:43:25 -03'00'