Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD DE ESCALACIÓN DE PRIVILEGIOS EN CISCO IOS XE

16/10/2023

CONTENIDO

INTRODUCCIÓN

Cisco es consciente de la explotación activa de una vulnerabilidad previamente desconocida en la función de interfaz de usuario web del software Cisco IOS XE cuando se expone a Internet o a redes que no son de confianza. Esta vulnerabilidad permite a un atacante remoto y no autenticado crear una cuenta en un sistema afectado con acceso de nivel de privilegio 15. A continuación, el atacante puede utilizar esa cuenta para hacerse con el control del sistema afectado.

VULNERABILIDAD DE ESCALACIÓN DE PRIVILEGIOS EN CISCO IOS XE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_10_16_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	16/10/2023
Es día cero (0 day):	No

RESUMEN

Cisco es consciente de la explotación activa de una vulnerabilidad previamente desconocida en la función de interfaz de usuario web del software Cisco IOS XE cuando se expone a Internet o a redes que no son de confianza. Esta vulnerabilidad permite a un atacante remoto y no autenticado crear una cuenta en un sistema afectado con acceso de nivel de privilegio 15. A continuación, el atacante puede utilizar esa cuenta para hacerse con el control del sistema afectado.

Cisco proporcionará actualizaciones sobre el estado de esta investigación y cuándo hay un parche de software disponible.

Esta vulnerabilidad afecta al software Cisco IOS XE si la función de interfaz de usuario web está habilitada. La función de interfaz de usuario web se habilita a través de los comandos **ip http server o ip http secure-server**

Para determinar si la función HTTP Server está habilitada para un sistema, inicie sesión en el sistema y utilice el comando **show running-config | include ip http server|secure|active** en la CLI para verificar la presencia del comando **ip http server o el comando ip http secure-server** en la configuración global. Si alguno de los comandos está presente, la función de servidor HTTP está habilitada para el sistema.

En el ejemplo siguiente se muestra el resultado del comando **show running-config | include ip http server|secure|active** para un sistema que tiene habilitada la función HTTP Server:

```
Router# show running-config | include ip http server|secure|active
ip http server
ip http secure-server
```

Nota: La presencia de uno o ambos comandos en la configuración del sistema indica que la función de interfaz de usuario web está habilitada.

Si el comando **ip http server** está presente y la configuración también contiene **ip http active-session-modules none**, la vulnerabilidad no se puede explotar 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 se puede explotar a través de HTTPS.

DETALLES

La interfaz de usuario web es una herramienta de administración del sistema basada en GUI integrada que proporciona la capacidad de aprovisionar el sistema, simplificar la implementación y la capacidad de administración del sistema y mejorar la experiencia del usuario. Viene con la imagen predeterminada, por lo que no es necesario habilitar nada ni instalar ninguna licencia en el sistema. La interfaz de usuario web se puede utilizar para crear configuraciones, así como para supervisar y solucionar problemas del sistema sin necesidad de tener experiencia en CLI.

La interfaz de usuario web y los servicios de administración no deben estar expuestos a Internet ni a redes que no sean de confianza.

INDICADORES DE COMPROMISO

Para determinar si un sistema puede haberse visto comprometido, realice las siguientes comprobaciones:

Compruebe los registros del sistema para ver si hay alguno de los siguientes mensajes de registro en los que el ***user*** podría ser **cisco_tac_admin, cisco_support** o cualquier usuario local configurado que sea 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
```

Nota: El mensaje **%SYS-5-CONFIG_P** estará presente para cada instancia en la que un usuario haya accedido a la interfaz de usuario web. El indicador que hay que buscar son los nombres de usuario nuevos o desconocidos presentes en el mensaje.

Compruebe los registros del sistema para ver si aparece el siguiente mensaje en el que ***filename*** es un nombre de archivo desconocido que no se correlaciona con una acción de instalación de archivos esperada:

```
%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD filename
```

Cisco Talos ha proporcionado el siguiente comando para verificar la presencia del implante donde ***systemip*** es la dirección IP del sistema que se va a verificar. Este comando debe emitirse desde una estación de trabajo con acceso al sistema en cuestión:

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

Si la solicitud devuelve una cadena hexadecimal, el implante está presente.

Nota: Si el sistema está configurado solo para acceso HTTP, utilice el esquema HTTP en el ejemplo de comando.

Los siguientes identificadores de regla de Snort también están disponibles para detectar explotaciones:

- 3:50118:2 – puede alertar para la inyección inicial del implante
- 3:62527:1 – puede alertar sobre la interacción del implante
- 3:62528:1 – puede alertar sobre la interacción del implante
- 3:62529:1 – puede alertar sobre la interacción del implante

RECOMENDACIONES

Cisco recomienda encarecidamente que los clientes deshabiliten la función de servidor HTTP en todos los sistemas orientados a Internet. Para deshabilitar la función de servidor HTTP, utilice el comando **no ip http server o no ip http secure-server** en el modo de configuración global. Si tanto el servidor HTTP como el servidor HTTPS están en uso, ambos comandos son necesarios para deshabilitar la función de servidor HTTP.

El siguiente árbol de decisión se puede usar para ayudar a determinar cómo evaluar un entorno e implementar protecciones:

- ¿Está ejecutando IOS XE?
    - **No**. El sistema no es vulnerable. No es necesario realizar ninguna otra acción.
    - **Sí**. ¿Está configurado **ip http server o ip http secure-server**?
        - **No**. La vulnerabilidad no es explotable. No es necesario realizar ninguna otra acción.
        - **Sí**. ¿Ejecuta servicios que requieren comunicación HTTP/HTTPS (por ejemplo, eWLC)?
            - **No**. Deshabilite la función de servidor HTTP.
            - **Sí**. Si es posible, restrinja el acceso a esos servicios a redes de confianza.

Al implementar controles de acceso para estos servicios, asegúrese de revisar los controles, ya que existe la posibilidad de que se produzca una interrupción en los servicios de producción. Si no está seguro de estos pasos, trabaje con su organización de apoyo para determinar las medidas de control adecuadas.

Después de implementar los cambios, utilice el comando **copy running-configuration startup-configuration** para guardar la **running-configuration**. Esto asegurará que los cambios no se reviertan en caso de una recarga del sistema.
Cisco es consciente de la explotación activa de esta vulnerabilidad.
Esta vulnerabilidad se encontró durante la resolución de varios casos de soporte del TAC de Cisco.

RECOMENDACIONES

Ya que aun no existe un parche para esta vulnerabilidad las recomendaciones iniciales son:

- Deshabilitar la función de servidor HTTP en todos los sistemas orientados a Internet.
- Comprobar los logs del sistema como:
    - Inicios de sesiones.
    - Acciones realizadas.
    - Archivos creados.
- Validar si existen conexiones o solicitudes de IPs desconocidas.
- Si es posible, restrinja el acceso a esos servicios a redes de confianza.
- Instalar la actualización cuando sea lanzada por Cisco

Cisco proporcionará actualizaciones sobre el estado de esta investigación y cuándo hay un parche de software disponible.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-de-escalacion-de-privilegios-en-cisco-ios-xe/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente