BOLETÍN DE ALERTA

Boletín Nro.: 2023-03
Fecha de publicación: 13/01/2023
Tema: Vulnerabilidades de omisión de autenticación y ejecución de comandos arbitrarios en productos Cisco.

Los productos afectados son:

- Enrutadores Cisco RV016 Multi-WAN VPN.
- Enrutadores Cisco RV042 Dual WAN VPN.
- Enrutadores Cisco RV042G Dual Gigabit WAN VPN.
- Enrutadores Cisco RV082 Dual WAN VPN.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre dos vulnerabilidades con *PoC* pública que afectan a enrutadores Cisco, que permitirían a un atacante obtener acceso no autorizado al sistema y provocar ejecución de comandos.

Las vulnerabilidades reportadas se componen de 1 (una) de severidad "Crítica" y 1 (una) de severidad "Media". Las mismas se detallan a continuación:

- CVE-2023-20025, de severidad "Crítica", con puntuación de 9.0. Esta vulnerabilidad se debe a una validación incorrecta de entradas del usuario en paquetes *HTTP* de la interfaz de administración web de enrutadores Cisco Small Business. Esto permitiría a un atacante remoto no autenticado realizar omisión de autenticación web y obtener accesos como *root* a través de una solicitud *HTTP* especialmente diseñada.

- CVE-2023-20026, de severidad "Media", con puntuación de 6.5. Esta vulnerabilidad se debe a la validación incorrecta de entradas de los usuarios en paquetes *HTTP*. Esto permitiría a un atacante remoto autenticado con credenciales administrativas realizar ejecución arbitraria de comandos y obtener privilegios de *root* en el dispositivo afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante obtener acceso no autorizado al sistema y provocar ejecución de comandos, como usuario *root*.

Mitigación:

Si bien Cisco no ha lanzado actualizaciones aún, recomendamos seguir los siguientes pasos de mitigación ofrecidos por el fabricante:

1. Deshabilitar el administrador remoto:
    a. Iniciar sesión en la interfaz de administración del dispositivo.

b. Elegir **Firewall > General**.
c. Desactivar **Administración remota**.

2. Bloquear el acceso a los puertos 443 y 60443, agregando un nuevo servicio a las reglas de acceso del dispositivo para el puerto 60443. No es necesario crear un servicio para el puerto 443 porque está predefinido en la lista de servicios.
   a. Iniciar sesión en la interfaz de administración del dispositivo.
   b. Elegir **Firewall > Reglas de acceso**.
   c. Hacer clic **Administración de servicios**.
   d. En **Nombre de servicio**, escribir TCP-60443.
   e. En la lista desplegar **Protocolo**, elegir **TCP**.
   f. En ambos campos **Intervalo de puertos**, escribir 60443.
   g. Hacer clic en **Agregar a la lista** y **Aceptar**.

3. Crear reglas de acceso para bloquear los puertos 443 y 60443
   a. Iniciar sesión en la interfaz de administración del dispositivo.
   b. Hacer clic en **Agregar**.
   c. En la lista desplegar **Acción**, elegir **Denegar**.
   d. En la lista desplegar **Servicio**, elegir **HTTPS (TCP 443-443)**.
   e. En la lista desplegar **Log**, elegir **Log packets match this rule (Los paquetes de registro coinciden con esta regla).**
   f. En la lista desplegar **Interfaz de origen**, elegir la opción que coincida con la conexión WAN del dispositivo.
   g. En la lista desplegar **IP de origen**, elegir **Cualquiera**.
   h. En la lista desplegar **IP de destin**o, elegir **Single**.
   i. En ambos campos IP de **destino**, introducir la **dirección IP** de **WAN**.
   j. Hacer clic en **Guardar**.
   k. Para crear una regla de acceso para el puerto 60443, repita los pasos anteriores, pero para el **paso 5**, elegir **HTTPS (TCP 60443-60443)** en la lista desplegable **Servicio**.

Nota: Si se utiliza un segundo puerto **WAN**, es necesario configurar dos reglas **ACL** adicionales, utilizando el número **WAN** y la **dirección IP** para el segundo puerto.

Adicionalmente, recomendamos analizar la posibilidad de reemplazar los equipos RV016, RV042, RV042G y RV082 por otros que tengan soporte a futuro, debido a que estos modelos se encuentran ya en fase de *End of life (EoL)* y no recibirán parches para futuras vulnerabilidades.

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20025
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20026