# Vulnerabilidades en Cisco Adaptive Security Appliance y Firepower Threat Defense

CYBERZAINTZA-AVISOS

**TLP: CLEAR**

www.ciberseguridad.eus

## TABLA DE CONTENIDO



## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## 1. Resumen ejecutivo

**Cisco** ha publicado avisos de seguridad para tratar **2 vulnerabilidades** de **severidad alta** cuyos identificadores son CVE-2024-20353 y CVE-2024-20359, que afectan a los productos **Cisco Adaptive Security Appliance y Firepower Threat Defense.**

Cisco ha confirmado que **estas vulnerabilidades han sido objeto de explotación**, recomendando a sus clientes que actualicen el software a la versión corregida para resolverlas. Además, se insta a monitorizar los registros del sistema en busca de posibles indicadores de cambios no documentados en la configuración, reinicios no programados y cualquier actividad anómala relacionada con credenciales, ya que, dicha explotación supone una **amenaza de alta gravedad para la confidencialidad y la integridad** de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

## 2. Recursos afectados

Estarán afectadas por la vulnerabilidad CVE-2024-20353 aquellas versiones de Cisco ASA y FTD si tienen una o más de las configuraciones vulnerables. A continuación, se enumeran las características del software, así como la configuración posiblemente vulnerable del mismo.

En el caso de Cisco ASA se tiene:

- Acceso remoto AnyConnect IKEv2:
  - crypto ikev2 enable [...] client-services port.
- Local Certificate Authority (CA):
  - crypto ca server,
  - no shutdown.
- Management Web Server Access (including ASDM and CSM):
  - http server enable
  - http.
- Mobile User Security (MUS):
  - webvpn
  - mus password
  - mus server enable port
  - mus
- REST API:
  - rest-api image disk0:/rest-api agent
- SSL VPN:
  - Webvpn
  - Enable

En el caso del software FTD (Firepower Threat Defense) se tiene:

- Acceso remoto AnyConnect IKEv2:
  - crypto ikev2 enable [...] client-services port.
- AnyConnect SSL VPN.

- Webvpn
- Enable

- HTTP server enabled.

  - http server enable.
  - http

Los recursos afectados por la vulnerabilidad CVE-2024-20359 serán aquellos productos Cisco que estén ejecutando una versión vulnerable del software Cisco ASA o FTD. No se requiere una configuración específica.

## 3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2024-20353: vulnerabilidad en los servidores de gestión y VPN para el software **Cisco Adaptive Security Appliance (ASA)** y el software **Cisco Firepower Threat Defense (FTD)**, cuya explotación podría permitir a un atacante remoto no autenticado provocar la recarga inesperada del dispositivo, este hecho conduciría a una condición de denegación de servicio DoS. El origen de la vulnerabilidad radica en una comprobación de errores incompleta al analizar un encabezado HTTP.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 835: Loop with Unreachable Exit Condition (Infinite Loop)

CVSS Base: **8.6**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

CVE-2024-20359: vulnerabilidad en una capacidad heredada que permite la precarga de clientes VPN y complementos, y que ha estado disponible en el software **Cisco Adaptive Security Appliance (ASA)** y el software **Cisco Firepower Threat Defense (FTD)**. La explotación de esta vulnerabilidad podría permitir a un atacante local, autenticado, ejecutar código arbitrario con privilegios de root. Se requieren privilegios de administrador para explotar esta vulnerabilidad.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 94: Improper Control of Generation of Code (Code Injection)

CVSS Base: **6.0**

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**

- **Integridad: Alta**
- **Disponibilidad:** Ninguna

## 4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En el caso de las vulnerabilidades CVE-2024-20353 y CVE-2024-20359 Cisco ha lanzado actualizaciones de software gratuitas que abordan los fallos descritos en este aviso. Los clientes con contratos de servicio que les otorgan actualizaciones de software regulares deben obtener correcciones de seguridad a través de sus canales de actualización habituales.

## 5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-20353.
- CVE-2024-20359.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY