Nro. Alerta:	AL-2024-028	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	14-nov-2024	**VULNERABILIDAD CISCO ASA Y FTD**	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Fuerza bruta

Nivel de riesgo: Alto

II. ALERTA

Cisco advierte sobre una vulnerabilidad de día cero identificada como **CVE-2023-20269** y con puntaje **CVSS** de **5.0** en sus equipos Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD), la misma es explotada de forma continua por operaciones de ransomware para obtener acceso inicial a las redes corporativas.

Figura 1.- *Ilustración asociada a Cisco* ***Fuente: Cisco DRA***

III. INTRODUCCIÓN

Una vulnerabilidad en el módulo de criptografía de software del software Cisco Adaptive Security Appliance (ASA) y el software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto autenticado o un atacante no autenticado en una posición de intermediario provoque un error inesperado en la recarga del dispositivo que resulta en una condición de denegación de servicio (DoS).

La vulnerabilidad se debe a un error lógico en la forma en que el módulo de criptografía de software maneja tipos específicos de errores de descifrado. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes maliciosos a través de una conexión IPsec establecida. Un exploit exitoso podría hacer que el dispositivo se bloquee y obligarlo a recargarse. La explotación exitosa de esta vulnerabilidad no comprometerá ningún dato cifrado.

Nota: Esta vulnerabilidad afecta únicamente a la versión 9.16.1 del software Cisco ASA y la versión 7.0.0 del software Cisco FTD.

IV. VECTOR DE ATAQUE.

Ataque de fuerza bruta

El ataque de fuerza bruta puede ejecutarse si se cumplen todas las siguientes condiciones:

1. Al menos un usuario está configurado con una contraseña en la base de datos LOCAL o la autenticación de gestión HTTPS apunta a un servidor AAA válido.
2. La VPN SSL está habilitada en al menos una interfaz o la VPN IKEv2 está habilitada en al menos una interfaz.

Establecimiento no autorizado de sesión VPN SSL sin cliente

Para establecer con éxito una sesión VPN SSL sin cliente, deben cumplirse todas las siguientes condiciones:

1. El atacante dispone de credenciales válidas para un usuario presente en la base de datos LOCAL o en el servidor AAA utilizado para la autenticación de gestión HTTPS. Estas credenciales podrían obtenerse mediante técnicas de ataque de fuerza bruta.

2. El dispositivo ejecuta el software Cisco ASA versión 9.16 o anterior.
3. VPN SSL habilitado en al menos una interfaz.
4. El protocolo SSL VPN sin cliente está permitido en la DfltGrpPolicy.

Este ataque no afecta al software Cisco FTD pues no cuenta con la característica SSL VPN sin cliente.

V. INDICADORES DE COMPROMISO

Los detalles de las vulnerabilidades 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

VI. IMPACTO:

Los productos afectados, son los siguientes:

- Productos CISCO con versiones de software vulnerable:
  - ✓ ASA (*Adaptive Security Appliance*)
  - ✓ FTD (*Firepower Threat Defense*)
  - ✓ FMC (*Firepower Management Center*)
- CISCO ASA y FTD
  - ✓ que tienen configurado el modo de cortafuegos transparente;
  - ✓ con una configuración vulnerable de AnyConnect o WebVPN.
- CISCO FTD que utilizan versiones del proyecto Snort3 de prevención de intrusiones (IPS) de código abierto anteriores a la 3.1.0.100 con configuraciones de reglas específicas.

VII. RECOMENDACIONES:

Cisco publicará una actualización de seguridad para abordar la vulnerabilidad CVE-2023-20269, pero hasta que las correcciones estén disponibles, se recomienda a los administradores del sistema que tomen las siguientes medidas:

- Cisco ha publicado actualizaciones y, en algunos casos soluciones alternativas, que abordan las vulnerabilidades descritas en este aviso.
- 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. 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.
- Utilizar DAP (Dynamic Access Policies) para detener los túneles VPN con DefaultADMINGroup o DefaultL2LGroup.
- Denegar el acceso con Default Group Policy ajustando vpn-simultaneous-logins para DfltGrpPolicy a cero, y asegurándose de que todos los perfiles de sesión VPN apuntan a una política personalizada.
- Implemente las restricciones de la base de datos de usuarios LOCAL bloqueando usuarios específicos a un único perfil con la opción ‘group-lock’, y evite las configuraciones de VPN ajustando ‘vpn-simultaneous-logins’ a cero.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-de-dia-cero-en-vpn-de-cisco-asa-y-ftd/
- https://netglobalis.com/ciberseguridad-vulnerabilidad-cisco-firepower-threat-defense/
- https://netebu.com/announcements/266/Varias-vulnerabilidades-en-dispositivos-ASA-FTD-y-FMC-de-CISCO.html
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-3
- https://www.cisco.com/c/es_mx/support/docs/security/adaptive-security-appliance-asa-software/217663-troubleshoot-asa-or-ftd-unexpected-reloa.html
- https://www.ciberseguridad.eus/sites/default/files/2024-04/Cyberzainta_Avisos_Vulnerabilidades_Cisco_CSA_yFTD_TLPCLear_v3.pdf