BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-58
Fecha de publicación: 24/10/2024
Tema: Vulnerabilidades críticas en productos Cisco
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Cisco FMC (Firepower Management Center), afecta a todas las versiones actuales.
- Cisco ASA (Adaptive Security Appliance)
- Cisco FTD (Firepower Threat Defense) versiones de 7.1 a 7.4 con DB 387 o inferior. Modelos afectados: 1000, 2100, 3100 y 4200 series.

Descripción

Cisco ha anunciado recientemente que han identificado varias vulnerabilidades críticas y han lanzado actualizaciones para mitigar estas fallas de seguridad que han sido activamente explotadas en varias de sus tecnologías: Cisco ASA (Adaptive Security Applience), dispositivo de seguridad que combina funciones de firewall, antivirus, prevención de intrusiones y red privada virtual (VPN); Cisco FMC (Firepower Management Center), el centro de administración de firewall seguro de Cisco; y Cisco FTD (Firepower Threat Defense) solución de seguridad que identifica patrones de tráfico de red, crea alertas, y controla la red.

Las vulnerabilidades más importantes son las siguientes:

1. CVE-2024-20424 (CVSS de 9.9): Esta vulnerabilidad permite a un atacante remoto autenticado ejecutar comandos arbitrarios en el sistema operativo con privilegios de root. La falla se origina en una validación insuficiente de las entradas en ciertas solicitudes HTTP dentro de la interfaz de gestión web de Cisco FMC, lo que permite que un atacante que se autentique en dicha interfaz envíe una solicitud HTTP manipulada y así elevar su acceso, incluso desde cuentas de usuario de bajo nivel para ejecutar comandos privilegiados en el sistema, lo que podría llevar a un control total del dispositivo.

2. CVE-2024-20412 (CVSS de 9.3): Esta vulnerabilidad, con una puntuación CVSS de 9.3, permite a atacantes locales no autenticados explotar credenciales estáticas incrustadas en el sistema, lo que podría resultar en acceso no autorizado y cambios en la configuración. El problema central radica en la presencia de cuentas estáticas con contraseñas codificadas dentro de los sistemas de Cisco Firepower afectados. Estas cuentas permiten a un atacante con acceso local eludir las medidas de autenticación y acceder a la interfaz de línea de comandos (CLI) del dispositivo utilizando credenciales estáticas. Una vez autenticado, el atacante puede ejecutar comandos limitados, recuperar información sensible o incluso hacer que el dispositivo se vuelva inarrancable al modificar ciertas opciones de configuración.

3. CVE-2024-20481 (CVSS de 5.8): Esta vulnerabilidad permite a los atacantes lanzar ataques de denegación de servicio (DoS) contra los servicios de VPN de Acceso Remoto (RAVPN) en dispositivos que ejecutan versiones vulnerables del software ASA o FTD con RAVPN habilitado, con una puntuación CVSS de 5.8 que indica un nivel moderado de severidad; esta vulnerabilidad se debe a un problema de agotamiento de recursos, ya que un atacante puede enviar numerosas solicitudes de autenticación VPN, lo que agota los recursos del dispositivo y provoca la denegación del servicio RAVPN.

Solución

Cisco ha lanzado actualizaciones de software que solucionan estas vulnerabilidades y recomienda los usuarios a actualizar a una versión corregida lo antes posible. Es fundamental que los administradores de sistemas actualicen de inmediato a las versiones corregidas para prevenir ataques, ya que la explotación de esta vulnerabilidad puede resultar en una total toma de control del sistema. Para más información visite Cisco.com

Información adicional:

- CVE-2024-20424 (CVSS 9.9): Cisco FMC Software Vulnerability Grants Attackers Root Access
- Active Exploits Target Cisco ASA and FTD VPNs: Urgent Update Needed (CVE-2024-20481)
- CVE-2024-20412: Unauthorized Access to Cisco Firepower Devices via Static Credentials

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com