BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-11
Fecha de publicación: 27/05/2024
Tema: Actualización de seguridad crítica para Cisco FMC, ASA y FTD
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Firepower Management Center (FMC).
- Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower Threat Defense (FTC).

Descripción:

Cisco abordó un conjunto de vulnerabilidades conocidas como CVE-2024-20355, CVE-2024-20363, CVE-2024-20261, CVE-2024-20361, CVE-2024-20293 y CVE-2024-20360, siendo esta última la más crítica, con una puntuación de severidad de 8.8.

Estas vulnerabilidades se encuentran en los productos Cisco ASA, FTD y FMC. La vulnerabilidad que supone más riesgo reside en la interfaz de administración web de FMC y es una vulnerabilidad de inyección de SQL, un atacante puede manipular las consultas SQL de manera a obtener datos de la base de datos, ejecutar comandos del sistema donde reside el software así como realizar una elevación de privilegios; para explotar esta vulnerabilidad el atacante requiere previamente las credenciales de algún usuario con permisos de lectura en la interfaz de administración.

Cabe recalcar que, por el momento, no se ha registrado ninguna explotación hasta el día de hoy de esta vulnerabilidad. El parche recientemente publicado mitiga ésta y las demás vulnerabilidades mencionadas, incluso aquellas que se vieron envueltas en la campaña de ataque conocida como ArcaneDoor, que se enfocaba en vulnerar Cisco ASA y FTD para implantar malware, ejecutar comandos y exfiltración de datos en los dispositivos comprometidos.

Impacto

Un actor malintencionado que ya haya ganado acceso a la red puede explotar estas vulnerabilidades para manipular la base de datos local, así como la ejecución de comandos maliciosos, así, obteniendo persistencia en el equipo donde esté alojado FMC, teniendo la posibilidad del aumentar su capacidad de atacar a la red interna.

Además, las vulnerabilidades con severidad media mencionadas anteriormente, se relacionan con la elusión de reglas o configuraciones de los aplicativos, que podrían permitir a un atacante evadirlas.

Solución

Aplicar el parche oficial publicado por Cisco

Información adicional:

- https://securityaffairs.com/163718/security/a-high-severity-vulnerability-affects-cisco-firepower-management-center.html?
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs
- https://nvd.nist.gov/vuln/detail/CVE-2024-20360
- https://www.recordedfuture.com/vulnerability-database/CVE-2024-20360
- Cisco Event Response: Attacks Against Cisco Firewall Platforms
- Cisco Event Response: May 2024 Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com