I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: Alto

II. ALERTA

Se han detectado vulnerabilidades en el acceso remoto VPN de CISCO ASA (Adaptative Security Appliance) y CISCO FTD (Firepower Threat Defense) que permitirían a un atacante ejecutar de manera remota ataques de fuerza bruta y establecer conexiones SSL VPN, con la finalidad de instalar ransomware.

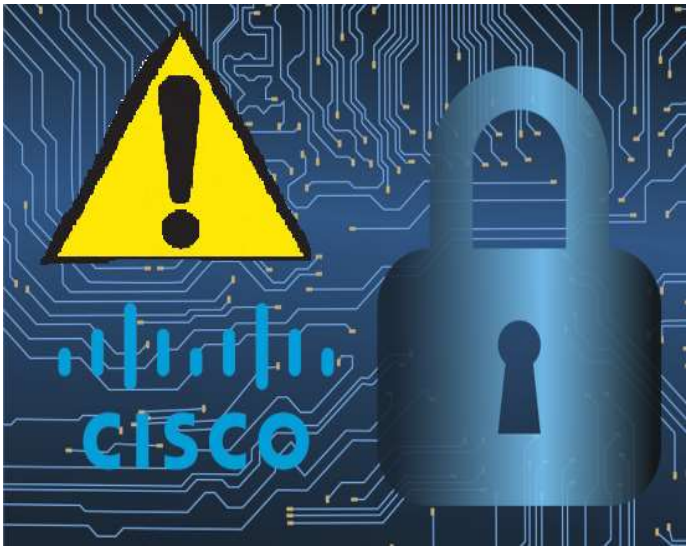

Figura 1.- lustración relacionada a vulnerabilidades CISCO ASA
Fuente: Elaboración Propia

III. INTRODUCCIÓN

Investigadores han detectado vulnerabilidades en las plataformas de seguridad de CISCO, Adaptative Security Appliance (CSA) y Firepower Threat Defender (FTD), que permitirían a un atacante remoto ejecutar técnicas de fuerza bruta y generación de sesiones SSL VPN a través de cuentas de usuario no autorizadas. El objetivo inicial es obtener cuentas de usuario existentes y posteriormente a través de una conexión de tipo default instalar programas ransomware para bloquear el acceso a sistemas y activos de información vinculados a los productos CISCO.

CISCO ASA es el sistema operativo para los productos ASA, y provee capacidades de firewall para diversos tipos de arquitecturas de red. CISCO FTD es una herramienta integral que permite la generación de alertas y control de red.

Los dispositivos CISCO afectados son aquellos que mantienen instaladas las aplicaciones vulnerables. Las características técnicas específicas de la explotación de las vulnerabilidades detectadas, se encuentran registradas en el formulario de priorización de riesgos CVE, CVE-2023-20269

IV. VECTOR DE ATAQUE:

- Conexiones remotas desde la red de Internet

V. IMPACTO:

- Instalación de Ransomware
- Instalación no autorizada de aplicaciones.
- Identificación de usuarios existentes y validados.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Ejecutar las medidas de mitigación emitidas por el desarrollador CISCO.
- Aislar secciones críticas de red en consideración a la criticidad y sensibilidad de los activos de información vinculados a los dispositivos de seguridad vulnerables.
- Aplicar el principio de menor privilegio en la creación de perfiles de usuario.
- Utilizar múltiples factores de autenticación.
- Implementar reglas de denegación de conexión hacia dispositivos vulnerables

VII. REFERENCIAS:

- CISCO. Cisco Adaptative Security Applicane Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability. (06/11 de 09 de 2023). Obtenido de https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
- NIST. CVE-2023-20269. (04 de 09 de 2023). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20269