Alerta de seguridad cibernética	9VSA20-00277-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de julio de 2020
Última revisión	23 de julio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a una vulnerabilidad que afectan a sus servicios de interface web Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD). El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-3452

Cve-2020-3452

Impacto

Una vulnerabilidad en la interfaz de servicios web del software Cisco Adaptive Security Appliance (ASA) y del software Cisco Firepower Threat Defense (FTD) de Cisco podría permitir que un atacante remoto no autenticado realice ataques transversales de directorio y lea archivos confidenciales en un sistema específico.

La vulnerabilidad se debe a la falta de una validación de entrada adecuada de las URL en las solicitudes HTTP procesadas por un dispositivo afectado. Un atacante podría explotar esta vulnerabilidad enviando una solicitud HTTP diseñada que contenga secuencias de caracteres transversales de directorio a un dispositivo afectado. Una explotación exitosa podría permitir al atacante ver archivos arbitrarios dentro del sistema de archivos de servicios web en el dispositivo objetivo.

El sistema de archivos de servicios web se habilita cuando el dispositivo afectado se configura con las funciones WebVPN o AnyConnect. Esta vulnerabilidad no se puede utilizar para obtener acceso a los archivos del sistema ASA o FTD o los archivos subyacentes del sistema operativo (SO).

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco si están ejecutando una versión vulnerable de Cisco ASA Software o Cisco FTD Software con una configuración vulnerable de AnyConnect o WebVPN.

En el enlace se puede verificar la configuración vulnerable según el software.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86