Cisco lanzó el miércoles 10 de agosto parches para contener múltiples fallas en su software, que podrían ser objeto de abuso para filtrar información confidencial en dispositivos susceptibles.

La vulnerabilidad, a la que se le asignó el identificador CVE-2022-20866 (puntaje CVSS: 7.4), se describió como un *«error lógico»* al manejar claves RSA en dispositivos que ejecutan el software Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD).

La explotación exitosa de la vulnerabilidad podría permitir que un atacante recupere la clave privada RSA por medio de un ataque de canal lateral de Lenstra contra el dispositivo objetivo.

> *«Si un atacante obtiene la clave privada RSA, podría usar la clave para hacerse pasar por un dispositivo que ejecuta el software Cisco ASA o el software Cisco FTD o para descifrar el tráfico del dispositivo»*, dijo Cisco en un aviso.

Cisco dijo que la vulnerabilidad afecta solo a las versiones 9.16.1 y posteriores del software Cisco ASA y las versiones 7.0.0 y posteriores del software Cisco FTD. Los productos afectados son los siguientes:

ASA 5506-X con servicios FirePOWER
ASA 5506H-X con servicios FirePOWER
ASA 5506W-X con servicios FirePOWER
ASA 5508-X con servicios FirePOWER
ASA 5516-X con servicios FirePOWER
Cortafuegos de última generación de la serie Firepower 1000
Dispositivos de seguridad de la serie Firepower 2100
Dispositivos de seguridad de la serie Firepower 4100
Dispositivos de seguridad de la serie Firepower 9300, y
Cortafuegos seguro 3100

Se lanzaron las versiones 9.16.3.19, 9.17.1.13 y 9.18.2 del software ASA y las versiones 7.0.4, 7.1.0.2-2 y 7.2.0.1 del software FTD para abordar la vulnerabilidad de seguridad.

Cisco le dio crédito a Nadia Heninger y George Sullivan de la Universidad de California en San Diego y a Jackson Sippe y Eric Wustrow de la Universidad de Colorado Boulder por reportar la vulnerabilidad.

Cisco también corrigió una vulnerabilidad de contrabando de solicitudes del lado del cliente en el componente Clientless SSL VPN (WebVPN) del software Cisco Adaptive Security Appliance (ASA) que podría permitir que un hacker remoto no autenticado realice ataques basados en navegador, como cross-site.

La compañía dijo que la vulnerabilidad, CVE-2022-20713 (puntuación CVSS: 4.3), afecta a los dispositivos Cisco que ejecutan una versión del software Cisco ASA anterior a la versión 9.17(1) y tienen activada la función Clientless SSL VPN.

Aunque no existen soluciones para corregir la vulnerabilidad, los usuarios afectados pueden deshabilitar la función Clientless SSL VPN, aunque Cisco advierte que hacerlo *«puede afectar negativamente la funcionalidad o el rendimiento de la red».*

El desarrollo se produce cuando la empresa de ciberseguridad Rapid7 reveló los detalles de 10 errores encontrados en ASA, Adaptive Security Device Manager (ASDM) y FirePOWER Services Software para ASA, siete de los cuales ya han sido abordados por Cisco.

Las vulnerabilidades incluyen CVE-2022-20829 (puntaje CVSS: 9.1), CVE-2022-20651 (puntaje CVSS: 5.5), CVE-2021-1585 (puntaje CVSS: 7.5), CVE-2022-20828 (puntaje CVSS: 6.5), y otras tres vulnerabilidades a las que no se les asignó un identificador CVE.