Cisco lanzó el miércoles 7 de septiembre parches para abordar tres vulnerabilidades de seguridad que afectan a sus productos, incluyendo una falla de alta gravedad revelada en NVIDIA Data Plane Development Kit (MLNX_DPDK) a fines del mes pasado.

Rastreada como CVE-2022-28199 (puntaje CVSS: 8.6), la vulnerabilidad se deriva de la falta de un manejo adecuado de errores en la pila de red de DPDK, lo que permite que un adversario remoto active una condición de denegación de servicio (DoS) y cause un impacto en integridad y confidencialidad de los datos.

> *«Si se observa una condición de error en la interfaz del dispositivo, el dispositivo puede recargarse o no recibir tráfico, lo que resulta en una condición de denegación de servicio (DoS)»,* dijo Cisco en un aviso.

DPDK se refiere a un conjunto de bibliotecas y controladores de tarjeta de interfaz de red (NIC) optimizados para el procesamiento rápido de paquetes, que ofrece un marco y una API común para aplicaciones de red de alta velocidad.

Cisco dijo que investigó su línea de productos y determinó que los siguientes servicios se vieron afectados por el error, lo que llevó al fabricante de equipos de red a lanzar actualizaciones de software:

- Software perimetral Cisco Catalyst 8000V
- Dispositivo virtual de seguridad adaptable (ASAv)
- Firewall seguro Threat Defense Virtual (anteriormente FTDv)

Además de CVE-2022-28199, Cisco también resolvió una vulnerabilidad en su software Cisco SD-WAN vManage que podría *«permitir que un atacante adyacente no autenticado que tenga acceso a la red lógica VPN0 también acceda a los puertos del servicio de mensajería en un sistema afectado».*

La compañía culpó de la deficiencia, a la que se le asignó el identificador CVE-2022-20696

(puntuación CVSS: 7.5), a la ausencia de *«mecanismos de protección suficientes»* en los puertos del contenedor del servidor de mensajería. Le dio crédito a Orange Business por informar sobre la vulnerabilidad.

La explotación exitosa de la falla podría permitir que el hacker vea e inyecte mensajes en el servicio de mensajería, lo que puede causar cambios en la configuración o hacer que el sistema se vuelva a cargar, agregó Cisco.

Una tercera vulnerabilidad corregida por Cisco es una falla en la interfaz de mensajería de la aplicación Cisco Webex (CVE-2022-20863, puntaje CVSS: 4.3), que podría permitir que un atacante remoto no autenticado modifique enlaces u otro contenido y realice ataques de phishing.

> *«Esta vulnerabilidad existe porque el software afectado no maneja correctamente la representación de caracteres. Un atacante podría explotar esta vulnerabilidad enviando mensajes dentro de la interfaz de la aplicación».*

Cisco le dio crédito a Rex, Bruce y Zachery del Binance Red Team, por descubrir y reportar la vulnerabilidad.

Finalmente, también reveló detalles de una vulnerabilidad de omisión de autenticación (CVE-2022-20923, puntaje CVSS: 4.0) que afecta a los enrutadores Cisco Small Business RV110W, RV130W, RV215W, que dijo que no se solucionará debido a que los productos están llegando al final de su vida útil (EOL).

«Cisco no ha lanzado y no lanzará actualizaciones de software para abordar la vulnerabilidad», dijo Cisco y sugiere a los usuarios *«migrar a los routers Cisco Small Business RV132W, RV160 o RV160W».*