Cisco lanzó actualizaciones de seguridad para abordar tres vulnerabilidades de alta gravedad en sus productos, que podrían explotarse para causar una condición de denegación de servicio (DoS) y tomar el control de los sistemas afectados.

La primera de las tres vulnerabilidades, CVE-2022-20783 (puntaje CVSS: 7.5), afecta el software Cisco TelePresence Collaboration Endpoint (CE) y el software Cisco RoomOS, y se debe a la falta de una validación de entrada adecuada, lo que permite que un atacante remoto no autenticado envíe tráfico especialmente diseñado a los dispositivos.

> *«Una explotación exitosa podría permitir que el atacante haga que el dispositivo afectado se reinicie normalmente o se reinicie en modo de mantenimiento, lo que podría resultar en una condición DoS en el dispositivo»,* dijo la compañía.

A la Agencia de Seguridad Nacional (NSA) de Estados Unidos se le atribuye el descubrimiento y notificación de la falla. El problema se solucionó en las versiones 9.15.10.8 y 10.11.2.2 del software Cisco Telepresence CE.

CVE-2022-20773 (puntuación CVSS: 7.5) es la segunda vulnerabilidad que se corregirá, se refiere a una clave de host SSH estática que está presente en Cisco Umbrella Virtual Applicane (VA), que ejecuta una versión de software anterior a la 3.3.2, lo que podría permitir que un atacante realice un ataque man-in-the-middel (MitM) en una conexión SSH y secuestre las credenciales del administrador.

La tercera vulnerabilidad de alta gravedad es un caso de escalada de privilegios en Cisco Virtualized Infraestructure Manager (CVE-2022-20732, puntuación CVSS: 7.8), que otorga a un atacante local autenticado el poder escalar privilegios en los dispositivos. Se resolvió en la versión 4.2.2 del software.

> *«Una explotación exitosa podría permitir que el atacante obtenga credenciales internas de la base de datos, que el atacante podría usar para ver y modificar el*

> *contenido de la base de datos. El atacante podría usar este acceso a la base de datos para elevar los privilegios en el dispositivo afectado»,* dijo la compañía.

Cisco también abordó 10 vulnerabilidades de gravedad media que abarcan su cartera de productos, incluyendo Webex Meeting, Unified Communications Products, Umbrella Secure Web Gateway y el software IOS XR.