Cisco Systems informó que no planea reparar una vulnerabilidad de seguridad crítica que afecta a algunos de sus routers para pequeñas empresas, sino que insta a los usuarios a reemplazar los dispositivos.

La vulnerabilidad, rastreada como CVE-2021-1459, tiene una puntuación CVSS de 9.8, y afecta al firewall VPN RV110W y a los routers RV130, RV130W y RV215W de pequeñas empresas, lo que permite que un atacante remoto no autenticado ejecute código arbitrario en un aparato afectado.

El error, que se debe a la validación incorrecta de la entrada proporcionada por el usuario en la interfaz de administración basada en la web, podría ser aprovechada por un actor malintencionado para enviar solicitudes HTTP especialmente diseñadas al dispositivo de destino y lograr la ejecución remota de código.

> *«Un exploit exitoso podría permitir al atacante ejecutar código arbitrario como usuario root en el sistema operativo subyacente del dispositivo afectado»*, dijo Cisco.

Al investigador de seguridad Treck Zhou, se le atribuye el crédito por informar sobre la vulnerabilidad. Aunque la compañía dijo que no ha habido evidencia de intentos de explotación activos en la naturaleza, no tiene la intención de lanzar un parche o poner a disposición ninguna solución alternativa, citando que los productos han llegado al final de su vida útil.

> *«Los enrutadores Cisco Small Business RV110W, RV130, RV130W y RV215W han entrado en el proceso de finalización de su vida útil. Se anima a los clientes a migrar a los enrutadores Cisco Small Business RV132W, RV160 o RV160W»,* dijo la compañía.

De forma separada, Cisco lanzó actualizaciones de software para abordar múltiples vulnerabilidades en el software Cisco SD-WAN vManage (CVE-2021-1137, CVE-2021-1479 y CVE-2021-1480), que podrían permitir que un atacante remoto no autenticado ejecute arbitrariamente código o permitir que un atacante local autenticado obtenga privilegios escalados en un sistema afectado.

Como consecuencia de una condición de desbordamiento de búfer, CVE-2021-1479 tiene una gravedad de 9.8 y una explotación exitosa de la cual *«podría permitir al atacante ejecutar código arbitrario en el sistema operativo subyacente con privilegios de root».*