Cisco lanzó el viernes correcciones para una vulnerabilidad de gravedad media, que afecta al software IOS XR que según la compañía, está siendo explotada en el mundo real.

Rastreada como CVE-2022-20821, con puntaje CVSS de 6.5, el problema se relaciona con una vulnerabilidad de puerto abierto, que podría ser abusada por un atacante remoto no autenticado para conectarse a una instancia de Redis y lograr la ejecución del código.

> *«Una explotación exitosa podría permitir que el atacante escriba en la base de datos en memoria de Redis archivos arbitrarios en el sistema de archivos del contenedor y recupere información sobre la base de datos de Redis»,* dijo Cisco.

> *«Dada la configuración del contenedor de espacio aislado en el que se ejecuta la instancia de Redis, un atacante remoto no podría ejecutar código remoto ni abusar de la integridad del sistema host del software Cisco IOS XR».*

La vulnerabilidad, que dijo que se identificó durante la resolución de un caso del centro de asistencia técnica (TAC), afecta a los routers de la serie Cisco 8000, que ejecutan el software IOS XR que tiene el RPM de verificación de estado instalado y activo.

La compañía también advirtió que se dio cuenta del intento de explotación de la vulnerabilidad de día cero a principios del mes.

> *«Cisco recomienda encarecidamente que los clientes apliquen soluciones alternativas adecuadas o actualicen a una versión de software reparada para corregir la vulnerabilidad».*