Cisco lanzó ayer los parches de seguridad para dos vulnerabilidades de alta gravedad, que afectan a su software IOS XR y que han estado siendo explotadas en la naturaleza al menos desde hace un mes.

Rastreadas como CVE-2020-3566 y CVE-2020-3569, las vulnerabilidades DoS no autenticadas de día cero, fueron detalladas por Cisco a fines del mes pasado, cuando la compañía descubrió que los hackers explotaban activamente el software Cisco IOS XR que está instalado en una variedad de dispositivos de la compañía.

Ambas vulnerabilidades DoS residían en la función del Protocolo de Enrutamiento de Multidifusión de Vector de Distancia (DVMRP) del software Cisco IOS XR, y existían debido a la implementación incorrecta de la administración de colas para los paquetes del Protocolo de Administración de Grupos de Internet (IGMP) en los dispositivos afectados.

IGMP es un protocolo de comunicación que suelen utilizar los hosts y los enrutadores adyacentes para utilizar de forma eficiente los recursos para las aplicaciones de multidifusión cuando se admite contenido de transmisión, como juegos y transmisión de video en línea.

> *«Estas vulnerabilidades afectan a cualquier dispositivo Cisco que esté ejecutando cualquier versión del software Cisco IOS XR si una interfaz activa está configurada bajo enrutamiento de multidifusión y está recibiendo tráfico DVMRP»,* dijo Cisco.
>
> *«Un administrador puede determinar si el enrutamiento de multidifusión está habilitado en un dispositivo emitiendo el comando show igmp interface»*.

La explotación exitosa de las dos vulnerabilidades podría permitir a los hackers remotos no autenticados, enviar paquetes IGMP especialmente diseñados a los dispositivos afectados para bloquear inmediatamente el proceso IGMP o agotar la memoria del proceso y eventualmente colapsar.

El consumo de memoria puede resultar negativamente en la inestabilidad de otros procesos que se ejecutan en el dispositivo, incluidos los protocolos de enrutamiento para redes internas y externas.

Las vulnerabilidades afectan a todos los dispositivos Cisco que ejecutan cualquier versión del software Cisco IOS XR, si una interfaz activa está configurada en enrutamiento de multidifusión y está recibiendo tráfico DVMRP.

En el momento en que Cisco inicialmente hizo públicas las vulnerabilidades, la compañía proporcionó algunas medidas de mitigación para resolver los problemas y bloquear los intentos de explotación activos, pero ahora, lanzó finalmente las actualizaciones de mantenimiento de software (SMU) para abordar las vulnerabilidades por completo.

> *«Aunque no hay soluciones para estas vulnerabilidades, existen múltiples mitigaciones disponibles para los clientes según sus necesidades»*, dijo la compañía.
>
> *«Al considerar las mitigaciones, debe entenderse que para el caso de agotamiento de la memoria, el limitador de velocidad y los métodos de control de acceso son efectivos. Para el caso de caída del proceso IGMP inmediato, solo el método de control de acceso es efectivo».*

Se recomienda a los clientes de Cisco que se aseguren de ejecutar la última versión del software Cisco IOS XR 6.6.3 o posterior.