Cisco informó sobre una vulnerabilidad en la función del Protocolo de Enrutamiento de Multidifusión Vectorial a Distancia (DVMRP) del software Cisco IOS XR, que podría permitir a un atacante remoto no autenticado, agotar la memoria de proceso de un dispositivo afectado.

La vulnerabilidad, rastreada como CVE-2020-3566 y con una puntuación CVSS de 8.6, se debe a una gestión insuficiente de cola para los paquetes del Protocolo de Gestión de Grupos de Internet (IGMP).

Un atacante podría aprovechar dicha vulnerabilidad al enviar tráfico IGMP diseñado a un dispositivo afectado.

> *«Un exploit exitoso podría permitir que el atacante agote la memoria, resultando en inestabilidad de otros procesos. Estos procesos pueden incluir, pero no se limitan a, protocolos de enrutamiento interior y exterior»,* dice la compañía en su aviso de seguridad.

La compañía asegura que lanzará actualizaciones de software para abordar la vulnerabilidad, pero por el momento no existen soluciones alternativas, aunque sí existen mitigaciones disponibles para los clientes según sus necesidades.

La vulnerabilidad afecta a cualquier dispositivo Cisco que ejecute cualquier versión del software Cisco IOS XR si una interfaz activa está configurada en enrutamiento de multidifusión.

Al explotar la vulnerabilidad, se obtiene como resultado el agotamiento de la memoria, lo que podría causar afectaciones a otros procesos del dispositivo. Es posible recuperar la memoria consumida por el proceso IGMP al reiniciar dicho proceso con el comando *process restart igmp*.

Cisco recomienda a los usuarios implementar un limitador de velocidad, como primera línea

de defensa. Esto requerirá que los clientes comprendan su tasa actual de tráfico IGMP y restablezcan una tasa más baja que la tasa promedio actual.

Como segunda línea de defensa, el usuario puede implementar una entrada de control de acceso (ACE) a una lista de control de acceso (ACL) de interfaz existente.

También es recomendable deshabilitar el enrutamiento IGMP para una interfaz donde no se necesita el procesamiento IGMP.

Cisco también informó que el 28 de agosto de 2020, el equipo de respuesta a incidentes de seguridad de productos CISCO (PSIRT), se percató del intento de explotación de la vulnerabilidad en la naturaleza.