Alerta de seguridad cibernética	9VSA20-00293-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de septiembre de 2020
Última revisión	02 de septiembre de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Cisco respecto a una vulnerabilidad en el manejo de paquetes IGMP que afecta la disponibilidad de los equipos. El presente informe incluye medidas de mitigación.

Vulnerabilidad

CVE-2020-3569

CVE-2020-3569

Una vulnerabilidad en “Distance Vector Multicast Routing Protocol” (DVMRP) podría permitir a un atacante remoto sin autenticar, botar inmediatamente el Internet Group Management Protocol (IGMP) o causar un agotamiento de memoria en él, causando un impacto negativo en otros procesos que estén siendo ejecutados en el dispositivo afectado.

Productos Afectados

Todos los productos Cisco que ocupen alguna versión del software Cisco IOS XR, con una interfaz activa configurada para ruteo multicast y que reciba tráfico DVMRP.

Un administrador podría determinar si el ruteo multicast está activado utilizando el comando *“show igmp interface”*. Si la respuesta está vacía, el ruteo no está activado y el producto no es vulnerable.
Un administrador podría determinar si el equipo recibe tráfico DVMRP utilizando el comando *"show igmp traffic"*. Si la entrada “DVMRP packets” contiene el valor 0 en la primera columna, y el contador sigue en cero en la siguiente ejecución del comando, el equipo no se encuentra recibiendo tráfico DVMRP.

Mitigaciones

No existen mitigaciones oficiales aún, pero se pueden aplicar múltiples medidas dependiendo de las necesidades de los usuarios.
Para mitigar el agotamiento de memoria, se recomiendo a los usuarios implementar un límite de tráfico IGMP, siendo este menor al promedio del actual.
Para mitigar ambos peligros (la caída inmediata o el agotamiento de memoria), los usuarios pueden implementar entradas de control de acceso (ACE) a una lista de control de acceso de interfaz existente. Alternativamente, el usuario puede crear una nueva lista de control de acceso para una interfaz específica que deniega el tráfico DVMRP entrante a la interfaz.
Para más detalles de la implementación de las medidas de mitigación, visitar enlace al final del documento.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3569