Cisco está emitiendo una advertencia sobre intentos de aprovechamiento de una vulnerabilidad de seguridad en su software IOS y IOS XE, lo que podría permitir que un atacante remoto autenticado logre la ejecución de código remoto en sistemas afectados.

Esta vulnerabilidad de nivel medio se identifica como CVE-2023-20109 y cuenta con una calificación CVSS de 6.6. Afecta a todas las versiones del software que tengan habilitado el protocolo GDOI o G-IKEv2.

La empresa menciona que la debilidad *«puede posibilitar que un atacante remoto autenticado, que tenga control administrativo sobre un miembro del grupo o un servidor de claves, ejecute código arbitrario en un dispositivo afectado o provoque que el dispositivo se bloquee».*

Asimismo, se resalta que el problema se origina debido a una validación insuficiente de atributos en los protocolos de Grupo de Dominio de Interpretación (GDOI) y G-IKEv2 de la función VPN GET, y podría ser explotado al comprometer un servidor de claves instalado o modificar la configuración de un miembro del grupo para que apunte a un servidor de claves controlado por el atacante.

Se informa que se descubrió esta vulnerabilidad tras una investigación interna y una revisión del código fuente que se llevó a cabo después de un *«intento de aprovechamiento de la función VPN GET».*

Esta revelación surge en un momento en que Cisco ha detallado un conjunto de cinco deficiencias en el Administrador de SD-WAN Catalyst (versiones 20.3 a 20.12) que podrían permitir que un atacante acceda a una instancia afectada o provoque una condición de denegación de servicio (DoS) en un sistema afectado:

- CVE-2023-20252 (calificación CVSS: 9.8) – Vulnerabilidad de Acceso no Autorizado
- CVE-2023-20253 (calificación CVSS: 8.4) – Vulnerabilidad de Reversión no Autorizada de la Configuración
- CVE-2023-20034 (calificación CVSS: 7.5) – Vulnerabilidad de Divulgación de

Información
- CVE-2023-20254 (calificación CVSS: 7.2) – Vulnerabilidad de Supresión de la Autorización
- CVE-2023-20262 (calificación CVSS: 5.3) – Vulnerabilidad de Denegación de Servicio

La explotación exitosa de estas fallas podría permitir que el actor de amenazas obtenga acceso no autorizado a la aplicación como un usuario no autorizado, evite la autorización y revierta las configuraciones del controlador, acceda a la base de datos Elasticsearch de un sistema afectado, entre otros, y provoque un bloqueo.

Se recomienda a los clientes actualizar a una versión de software corregida para remediar estas vulnerabilidades.