I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: Medio

II. ALERTA

Cisco muestra que han encontrado diferentes vulnerabilidades en su software IOS y en IOS XE que estaría permitiendo a un atacante remoto estar ejecutando código en los sistema afectados los cuales ponen en riesgo la integridad de los quipos ya que podrían causar un fallo en los mismos.

Figura 1.-lustración relacionada a vulnerabilidades en cisco.
Fuente: Elaboración Propia.

III. INTRODUCCIÓN

En una investigación interna se detectó la vulnerabilidad y se realizó una auditoria del código fuente la cual revelaría que el intento de explotación de la función GET VPN a la par esto se revela que cuando Cisco había detallado un conjunto de cinco fallas en Catalyst SD-WAN esto podría permitir que el atacante pueda generar un ataque de DoS o de plano acceder a una instancia ya afectada.

En la explotación éxitos a de los siguientes errores se podría permitir que el atacante pueda tener acceso no autorizado a la aplicación y de esta manera puede sobrepasar las configuraciones del control y pueda acceder incluso a la base de datos entre otras afecciones que se podría llegar a tener.

Además señaló que el problema se debe a una validación insuficiente de los atributos del dominio de interpretación del grupo (GDOI) y los protocolos G-IKEv2 de la función GET VPN. Podría convertirse en un arma comprometiendo un servidor de claves instalado o modificando las configuraciones de un miembro del grupo para apuntar a un servidor de clave controlado por un atacante.

Estas serán algunas de las vulnerabilidades que ya se han ido corrigiendo:

- CVE-2023-20252 (puntuación CVSS: 9,8): vulnerabilidad de acceso no autorizado
- CVE-2023-20253 (puntuación CVSS: 8,4): vulnerabilidad de reversión de configuración no autorizada
- CVE-2023-20034 (puntuación CVSS: 7,5): vulnerabilidad de divulgación de información
- CVE-2023-20254 (puntuación CVSS: 7,2): vulnerabilidad de omisión de autorización
- CVE-2023-20262 (puntuación CVSS: 5,3): vulnerabilidad de denegación de servicio

IV. VECTOR DE ATAQUE:

- Denegación de Servicios, Modificar código de manera arbitraria.

V. IMPACTO:

- Escalabilidad de privilegios.
- El atacante compromete el servidor de claves existente y tiene la capacidad de modificar los paquetes GDOI o G-IKEv2 que el servidor de claves envía al miembro del grupo.
- Creación de cuentas de usuario con perfiles administrativos.

VI. RECOMENDACIONES:

- Aislar productos que muestren un riesgo para los equipos que nos sea productos actualizados.
- Informar a usuarios respecto de amenazas provenientes en enlaces remitidos a través de correos electrónicos.
- Restringir la interacción con sitios web respecto de actividades de descarga y ejecución de archivos.

VII. REFERENCIAS:

- Software Cisco IOS e IOS XE. (27 de 09 de 2023). Obtenido de https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx
- NIST. CVE-2023-20109. (27 de 09 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-20109
- TheHackerNews Cisco(29 de 09 de 2023). Obtenido de https://thehackernews.com/2023/09/cisco-warns-of-vulnerability-in-ios-and.html