Cisco abordó una vulnerabilidad de máxima gravedad en su orquestador de sitios múltiples (MSO) de infraestructura centrada en aplicaciones (ACI), que podría permitir que un atacante remoto no autenticado eluda la autenticación en dispositivos vulnerables.

> *«Un atacante podría aprovechar esta vulnerabilidad mediante el envío de una solicitud hecha a mano a la API afectada. Un exploit exitoso podría permitir que el atacante reciba un token con privilegios de nivel de administrador que podría utilizarse para autenticarse en la API en MSO afectados y dispositivos Cisco Application Policy Infrastructure Controller (APIC) administrados»,* dijo la compañía.

La vulnerabilidad, rastreada como CVE-2021-1388, calificada con la máxima puntuación de 10 sobre 10 en el sistema de puntuación CVSS, se debe a una validación de token incorrecta en un punto final API de Cisco ACI MSO instalado en el motor de servicios de aplicaciones. Afecta a las versiones de ACI MSO que ejecutan una versión 3.0 del software.

ACI Multi-Site Orchestrator permite a los clientes monitorear y administrar las políticas de redes de acceso a las aplicaciones en todos los dispositivos Cisco APIC.

De forma separada, la compañía también corrigió varias vulnerabilidades en el motor de servicios de aplicaciones de Cisco (CVE-2021-1393 y CVE-2021-1396, con puntuación CVSS de 9.8), que podrían otorgar a un atacante remoto el acceso a un servicio privilegiado o API específicas, lo que resulta en capacidades para ejecutar contenedores o invocar operaciones a nivel de host y aprender *«información específica del dispositivo, crear archivos de soporte técnico en un volumen aislado y realizar cambios de configuración limitados».*

Ambas vulnerabilidades fueron el resultado de controles de acceso insuficientes para una API que se ejecuta en la red de datos, dijo Cisco.

La compañía dijo que las tres debilidades mencionadas se descubrieron durante las pruebas de seguridad internas, pero agregó que no detectó intentos maliciosos de explotación en la naturaleza.

Finalmente, Cisco corrigió una vulnerabilidad (CVE-2021-1361, puntuación CVSS de 9.8) en la implementación de un servicio de administración de archivos internos para los switches Cisco Nexus de la serie 3000 y los switches Cisco Nexus de la serie 9000 que ejecutan NX-OS, el sistema operativo de red de la empresa utilizado en sus conmutadores Ethernet de la marca Nexus.

Esto podría permitir que un atacante cree, elimine o sobrescriba archivos arbitrarios con privilegios de root en el dispositivo, dijo la compañía, incluyendo que el atacante pueda agregar una cuenta de usuario sin el conocimiento del administrador del dispositivo.

Cisco dijo que los switches Nexus 3000 y Nexus 9000 que ejecutan la versión 9.3 (5) o la versión 9.3 (6) del software Cisco NX-OS son vulnerables de forma predeterminada.

> *«Esta vulnerabilidad existe porque el puerto TCP 90/5 está configurado incorrectamente para escuchar y responder a las solicitudes de conexión externa. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes TCP diseñados a una dirección IP configurada en una interfaz local en el puerto TCP 9075»,* dijo Cisco.