BOLETÍN DE ALERTA

Boletín Nro.: 2021-05

Fecha de publicación: 03/03/2021

Tema: Múltiples vulnerabilidades en productos de Cisco.

Sistemas afectados:

- Cisco NX-OS Software versiones 9.3(5) o 9.3(6), presente en:
  - Nexus 3000 Series Switches,
  - Nexus 9000 Series Switches en modo NX-OS independiente.
- Cisco Application Services Engine Software, versiones 1.1 (3d) y anteriores.
- Cisco ACI Multi-Site Orchestrator (MSO) ejecutando una versión de software 3.0, solo si se desplegó en un Cisco Application Services Engine.

Descripción

Cisco ha informado sobre varias vulnerabilidad que se han identificado en sus productos, todas ellas de severidad crítica, que podrían permitir a un atacante remoto crear, borrar o modificar archivos aleatorios, obtener acceso privilegiado a información sensible u omitir la autenticación en el dispositivo afectado.

Una de las vulnerabilidades tiene gravedad **máxima** (CVSS **10**), identificada como CVE-2021-1388 afecta a su orquestador de sitios múltiples (MSO) de infraestructura centrada en aplicaciones (Cisco ACI MSO (Multi-Site Orchestrator)) y podría permitir que un atacante remoto no autenticado eluda la autenticación en dispositivos vulnerables.

Un atacante podría explotar esta vulnerabilidad enviando una petición, especialmente diseñada, a la API afectada. Una explotación exitosa podría permitir al atacante recibir un *token* con privilegios de nivel de administrador que podría ser utilizado para autenticarse en la API en los dispositivos MSO y Cisco APIC afectados.

La vulnerabilidad se debe a una validación incorrecta del token en un punto final de API específico y afecta a Cisco ACI MSO que ejecuta una versión 3.0 de software solo cuando se implementa en un Cisco ASE.

Las vulnerabilidades CVE-2021-1393 y CVE-2021-1396 de severidad **crítica** calificación CVSS **9,8**, que afectan a Cisco Application Services Engine, son vulnerabilidad de acceso no autorizado al servicio y acceso a la API del motor de servicios de aplicaciones de Cisco que podrían permitir que un atacante remoto no autenticado, a través de peticiones TCP y HTTP malformadas respectivamente, obtenga acceso privilegiado a operaciones a nivel de host o que obtenga información específica del dispositivo, cree archivos de diagnóstico y realice cambios de configuración limitados.

La vulnerabilidad CVE-2021-1361, severidad **crítica** calificación CVSS **9,8** que afecta a los switches Cisco Nexus de la serie 3000 y los switches Cisco Nexus de la serie 9000 que ejecutan NX-OS permite que un atacante remoto no autenticado cree, elimine o sobrescriba archivos arbitrarios con privilegios de root en el dispositivo

De acuerdo al fabricante, 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 9075 está configurado incorrectamente para escuchar y responder a solicitudes de conexión externa. pudiendo ser aprovechado esta vulnerabilidad para enviar paquetes TCP diseñados a una dirección IP configurada en una interfaz local en el puerto TCP 9075.

Además, se publicaron 5 vulnerabilidades de severidad Alta que se detallan a continuación:

- El CVE-2021-1368 severidad alta calificación 8,8 que afecta a Cisco FXOS y NX-OS. Vulnerabilidad de ejecución de código arbitrario y denegación de servicio de detección de enlace unidireccional. Un exploit exitoso podría permitir al atacante ejecutar código arbitrario con privilegios administrativos o hacer que el proceso UDLD de Cisco se bloquee y se reinicie varias veces, lo que provocaría que el dispositivo afectado se recargue y resulte en una condición DoS.
- El CVE-2021-1387 severidad alta calificación 8.6, que afecta a Cisco NX-OS IPv6 Netstack. Vulnerabilidad de denegación de servicio del software, podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.

- El CVE-2021-1230 severidad alta calificación 8.6 que afecta a ACI en Switches de estructura Cisco Nexus de la serie 9000 Vulnerabilidad de denegación de servicio de instalación de ruta BGP, podría permitir que un atacante remoto no autenticado provoque la caída de un proceso de enrutamiento, lo que podría conducir a una denegación de servicio (DoS).

- El CVE-2021-1227 severidad alta calificación 8.1 que afecta Cisco NX-OS. Vulnerabilidad de falsificación de solicitudes entre sitios NX-API, podría permitir que un atacante remoto no autenticado lleve a cabo un ataque de falsificación de solicitud entre sitios (CSRF) en un sistema afectado.

- El CVE-2021-1228 severidad alta calificación 7.4 que afecta a Cisco Nexus de la serie 9000. Vulnerabilidad de acceso no autorizado de VLAN de infraestructura de estructura de modo ACI en Switches que podría permitir que un atacante adyacente no autenticado eluda las validaciones de seguridad y conecte un servidor no autorizado a la VLAN de la infraestructura.

Mitigación

Cisco ha publicado parches de seguridad que corrigen las vulnerabilidades..Las actualizaciones de seguridad están disponibles en los siguientes enlaces.

- ACI (Application Centric Infrastructure) MSO ***ACTUALIZAR***.
- Cisco Nexus 3000 **ACTUALIZAR**.
- Cisco Nexus 9000 **ACTUALIZAR**.
- Motor de Servicios Cisco Application Services Engine ***ACTUALIZAR***.

Referencias

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3000-9000-fileaction-QtLzDRy2
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-case-mvuln-dYrDPC6w
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-authbyp-bb5GmBQv
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/811/
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-cisco-75