Boletín de alerta

Boletín Nro.: 48
Fecha de publicación: 27/05/2025
Tema: Alerta 2025-48 Vulnerabilidades críticas en productos Cisco
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Cisco ISE**,**
  - **Versiones anteriores al 3.3**
- Cisco Unified Intelligence Center (UIC),
  - **Versiones 12.5, 12.6 (antes de 12.5(1)SU ES04 y 12.6(2)ES04)**

Descripción

El equipo de Cisco identificó varias **vulnerabilidades críticas,** identificadas como **CVE-2025-20152,** la cual afecta en el procesamiento de mensajes RADIUS de Cisco Identity Services Engine (ISE)**; CVE-2025-20113 y CVE-2025-20114,** que son fallos de escalada de privilegios en Cisco Unified Intelligence Center (UIC), las cuales fueron reportadas recientemente y que permiten a los atacantes autenticados elevar privilegios o acceder a datos de otros usuarios debido a validaciones insuficientes de solicitudes API.

- **CVE-2025-20152**: Vulnerabilidad de denegación de servicio (DoS) en Cisco Identity Services Engine (ISE) relacionada con el procesamiento de mensajes RADIUS. Un atacante remoto no autenticado puede enviar solicitudes RADIUS especialmente diseñadas que causan una recarga completa del sistema, interrumpiendo la autenticación y el control de acceso en la red. Esta falla se debe a un manejo incorrecto de ciertas solicitudes RADIUS. De CVSS 3.1: 8.6 (Alta). No se ha reportado explotación activa.

- **CVE-2025-20113**: Vulnerabilidad de escalada de privilegios en Cisco Unified Intelligence Center (UIC). Un atacante autenticado puede elevar sus privilegios a nivel administrador para un conjunto limitado de funciones mediante la explotación de una validación insuficiente de parámetros suministrados por el usuario en solicitudes API o HTTP. Esto permite eludir controles de autorización. De CVSS 3.1: 7.1 (Alta).

- **CVE-2025-20114**: Vulnerabilidad de escalada horizontal de privilegios en Cisco UIC. Un atacante autenticado puede acceder a datos de otros usuarios mediante una referencia insegura directa a objetos debido a insuficiente validación de parámetros en solicitudes API. CVSS 3.1: 4.3 (Media).

Solución:

Recomendaciones y Medidas de Mitigación:

Las vulnerabilidades CVE-2025-20152, CVE-2025-20113 y CVE-2025-20114 afectan productos clave de Cisco y requieren atención inmediata para mitigar riesgos críticos.

- **Para CVE-2025-20152**, que impacta la función de procesamiento de mensajes RADIUS en Cisco Identity Services Engine (ISE), Cisco ha publicado un parche en la versión **ISE 3.4 Patch 1 (3.4P1)**. Más detalles y el parche oficial están disponibles en la Cisco Security Advisory.

- Para las vulnerabilidades **CVE-2025-20113 y CVE-2025-20114**, Cisco ha corregido estas fallas en las versiones **UIC 12.5(1)SU ES04** y **UIC 12.6(2)ES04**. Se recomienda actualizar a estas versiones o superiores cuanto antes. Más información y parches están en la Cisco Security Advisory para UIC.

Medidas adicionales recomendadas incluyen:

- Restringir el acceso a los sistemas afectados solo a redes y usuarios confiables.
- Implementar controles estrictos de autenticación y autorización para limitar la exposición.
- Monitorear activamente los registros de acceso, tráfico API y eventos del sistema para detectar posibles intentos de explotación.
- Segmentar la red para aislar los sistemas vulnerables y reducir la superficie de ataque.

Información adicional:

Múltiples vulnerabilidades en productos de Cisco | INCIBE-CERT | INCIBENVD – CVE-2025-32756

Cisco Identity Services Engine RADIUS Denial of Service Vulnerability

Cisco Unified Intelligence Center Privilege Escalation VulnerabilitiesCisco Patches High-Severity DoS, Privilege Escalation Vulnerabilities – SecurityWeek