BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-12
Fecha de publicación: 07/02/2025
Tema: Vulnerabilidades críticas en Cisco ISE
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Cisco Identity Services Engine (ISE) **versiones 3.0, 3.1, 3.2 y 3.3**

Descripción

Cisco ha identificado un par de vulnerabilidades críticas que permiten la ejecución de comandos como root y omisión de autorización en Cisco Identity Services Engine (ISE). Cisco ISE es una solución de software independiente para la administración de políticas de seguridad que proporciona acceso seguro a la red para usuarios y dispositivos, permitiendo la creación y aplicación de políticas de seguridad y acceso para dispositivos terminales conectados a los enrutadores y conmutadores de una organización. Las vulnerabilidades son:

- **CVE-2025-20124 (CVSS 9.9):** Esta vulnerabilidad se debe a una deserialización insegura de flujos de bytes Java proporcionados por el usuario en una API específica de Cisco ISE. Un atacante autenticado con credenciales administrativas de solo lectura podría explotar esta vulnerabilidad enviando un objeto Java serializado especialmente diseñado a la API afectada, lo que le permitiría ejecutar comandos arbitrarios con privilegios de root en el dispositivo comprometido.

- **CVE-2025-20125 (CVSS 9.1):** Esta vulnerabilidad surge de la falta de autorización en una API específica y de una validación inadecuada de los datos proporcionados por el usuario. Un atacante autenticado con credenciales administrativas de solo lectura podría aprovechar esta falla enviando una solicitud HTTP especialmente diseñada a la API afectada, lo que le permitiría obtener información sensible, modificar la configuración del sistema y reiniciar el dispositivo comprometido.

Solución

Cisco ha lanzado actualizaciones de software para abordar estas vulnerabilidades. Se recomienda a los administradores que actualicen sus implementaciones de Cisco ISE a las siguientes versiones corregidas:

- **Cisco ISE 3.1:** Actualizar a la versión 3.1P10.
- **Cisco ISE 3.2:** Actualizar a la versión 3.2P7.
- **Cisco ISE 3.3:** Actualizar a la versión 3.3P4.

Para más información, consulte el sitio oficial de Cisco.

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF
- CVE-2025-20124 (CVSS 9.9) & CVE-2025-20125 (CVSS 9.1): Cisco Patches Critical Flaws in Identity Services EngineCVE-2025-23114: Critical Code Execution Vulnerability in Veeam Backup Solutions Demands Immediate Action - Cybercory
- https://www.techmonitor.ai/technology/cybersecurity/cisco-critical-ise-security-flaws-administrators-update?cf-view

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com