BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-50
Fecha de publicación: 05/06/2025
Tema: Vulnerabilidad crítica en implementaciones en la nube de Cisco ISE
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Implementaciones de Cisco ISE en la nube*:

- En AWS: versiones 3.1, 3.2, 3.3 y 3.4
- En Azure: versiones 3.2, 3.3 y 3.4
- En Oracle Cloud Infraestructure: versiones 3.2, 3.3 y 3.4

* Obs.: Si la implementación de la administración primaria se encuentra on-premise, no se encuentra afectado
** Obs.: implementaciones on-premise o híbridos (appliance o virtual) no se encuentran afectadas; igualmente, implementaciones de ISE en las siguiente plataformas no se encuentran afectadas:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware cloud en AWS

Descripción

Cisco publicó una advertencia de seguridad crítica sobre una vulnerabilidad en el Cisco Identity Services Engine (ISE) cuando se despliega en plataformas de nube como AWS, Azure y OCI. Esta vulnerabilidad, identificada como CVE-2025-20286 y con un puntaje CVSS de 9.9 permite a un atacante remoto no autenticado acceder a datos sensibles y ejecutar operaciones administrativas limitadas.

Se trata de una vulnerabilidad en la manera en que se generan las credenciales, las cuales son estáticas, y por tanto, son las mismas entre diferentes implementaciones de Cisco ISE en la misma versión y plataforma.

Un atacante podría aprovechar esta vulnerabilidad extrayendo las credenciales de usuario de alguna instancia de Cisco ISE en la nube y luego utilizarlo para acceder a otras instancias similares, mediante puertos no securizados y expuestos.
Cisco ha publicado un parche para corregir esta vulnerabilidad. Si bien, no hay evidencia de explotación masiva, se ha publicado una prueba de concepto funcional.

Solución:

Para solucionar esta vulnerabilidad Cisco ha publicado un parche, hotfix ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz, válido para las versiones afectadas desde 3.1 hasta 3.4:

https://software.cisco.com/download/home/283801620/type/283802505/release/HP-CLOUD-CSCwn63400

Mitigación:

- Restrinja las direcciones IP de origen mediante grupos de seguridad en la nube
- Restrinja el acceso a través de la interfaz de usuario de ISE a direcciones IP de administrador conocidas
- Para instalaciones nuevas, ejecute el comando de reset-config para resetear la contraseña de usuario a un valor nuevo. Tenga en cuenta que restaurar un backup restaurará la contraseña original, conocida.

Información adicional:

Cisco Identity Services Engine on Cloud Platforms Static Credential Vulnerability

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.us

contact@cybolt.com

cybolt.com