# Boletín de alerta

**Boletín Nro.:** 61
**Fecha de publicación:** 17/07/2025
**Tema:** Alerta 2025-61 Vulnerabilidades RCE en productos de Cisco
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

- CVE-2025-20281 y CVE-2025-20337:
  - Cisco ISE e ISE-PIC – versiones 3.3 y 3.4, independientemente de la configuración del dispositivo.
- CVE-2025-20282:
  - Cisco ISE e ISE-PIC – versión 3.4, independientemente de la configuración del dispositivo. Esta vulnerabilidad no afecta a Cisco ISE e ISE-PIC versión 3.3 ni versiones anteriores.

## Descripción

Se han reportado vulnerabilidades críticas de tipo **ejecución remota de código (RCE)** no autenticado en la API de Cisco ISE de Cisco, las mismas se denominaron como: **CVE-2025-20282 (CVSSv3 10), CVE-2025-20281 (CVSSv3 10) y CVE-2025-20337 (CVSSv3 10).**

- CVE-2025-20281 y CVE-2025-20337: Vulnerabilidades de validación insuficiente de la entrada proporcionada por el usuario en Cisco ISE y Cisco ISE-PIC. Estas podrían permitir a un atacante remoto, no autenticado, ejecutar código arbitrario en el sistema operativo subyacente como *root*. El atacante no necesita credenciales válidas para explotar esta vulnerabilidad. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud de API manipulada.

- CVE-2025-20282: Vulnerabilidad de falta de comprobaciones de validación en Cisco ISE y Cisco ISE-PIC. Esta podría permitir a un atacante remoto, no autenticado, cargar archivos arbitrarios en un dispositivo afectado y luego ejecutar esos archivos en el sistema operativo subyacente como *root*. Un atacante podría explotar esta vulnerabilidad cargando un archivo manipulado en el dispositivo afectado.

Para ver el reporte completo del proveedor, puede dirigirse al siguiente enlace:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

# Solución:

El proveedor hay proveído parches de seguridad para corregir las vulnerabilidades:

| Versión de Cisco ISE o ISE-PIC | Primera versión corregida para CVE-2025-20281 | Primera versión corregida para CVE-2025-20282 | Primera versión corregida para CVE-2025-20337 |
|---|---|---|---|
| 3.2 y anteriores | No vulnerable | No vulnerable | No vulnerable |
| 3.3 | 3.3 Parche 7 | No vulnerable | 3.3 Parche 7 |
| 3.4 | 3.4 Parche 2 | 3.4 Parche 2 | 3.4 Parche 2 |

Para información de como actualizar sus productos, puede dirigirse a los siguientes enlace:

- https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu
- https://www.cisco.com/c/en/us/support/index.html

# Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6#vp
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-7?sstc=u88504nl570387