

Boletín de alerta

Boletín Nro.: 101

Fecha de publicación: 17/09/2026

Tema: Alerta 2026-101 Zero-day Crítico en Cisco ISE e ISE-PIC — CVE-2026-76460

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta a **Cisco ISE** y **Cisco ISE PIC**, independientemente de la configuración del dispositivo. Cisco ha publicado correcciones para las ramas soportadas siguientes:

Producto	Rama afectada	Versión corregida mínima
Cisco Identity Services Engine (ISE)	3.1	3.1 Patch 12
Cisco Identity Services Engine (ISE)	3.2	3.2 Patch 11
Cisco Identity Services Engine (ISE)	3.3	3.3 Patch 12
Cisco Identity Services Engine (ISE)	3.4	3.4 Patch 7
Cisco Identity Services Engine (ISE)	3.5 / 3.5.3	3.5 Patch 4
Cisco ISE Passive Identity Connector (ISE PIC)	Versiones vulnerables soportadas	Aplicar el patch equivalente de la rama desplegada

*Cisco ISE Software Release 3.0 llegó a **fin de mantenimiento de software**, por lo que no cuenta con una actualización de corrección para esta vulnerabilidad. Los equipos que permanezcan en esa rama deben planificar una actualización a una release soportada de forma prioritaria.

Descripción

Se publicado una vulnerabilidad **crítica** de bypass de autenticación en Cisco Identity Services Engine (**ISE**) y Cisco ISE Passive Identity Connector (**ISE PIC**), identificado como **CVE 2026 76460** con una puntuación **CVSS 10.0**, permite a un atacante remoto no autenticado enviar una solicitud especialmente diseñada a un endpoint API afectado, evadir la autenticación de la interfaz web de administración y obtener acceso no

autorizado al dispositivo. Cisco confirmó que la vulnerabilidad está siendo **explotada activamente**.

Dado que ISE suele actuar como componente central de control de acceso a red, autenticación y políticas de identidad, un compromiso puede afectar la administración de identidades, el acceso de usuarios y dispositivos a la red y la postura de seguridad de la organización. Se recomienda actualizar con prioridad máxima todos los nodos ISE/ISEPIC afectados y realizar una revisión de compromiso.

Cisco PSIRT confirmó conocimiento de explotación activa en entornos reales, aunque no ha publicado detalles sobre el actor responsable, el método exacto de ataque ni las organizaciones afectadas.

Cisco recomienda revisar el archivo `access.log` de ISE en busca de nombres de usuario sospechosos, en particular el usuario `dummyuser`. En entornos de despliegue distribuido, la revisión debe efectuarse en **cada nodo** de ISE/ISEPIC.`bleepingcomputer+1`

Ejecutar el siguiente comando en cada nodo:

```
admin#show logging application ise-kong/access.log | include dummyuser
```

La presencia de entradas relacionadas con `dummyuser` en el resultado debe tratarse como un **indicador de actividad maliciosa potencial** y requiere investigación inmediata.

Adicionalmente, se recomienda investigar:

- Inicios de sesión, sesiones API y cambios administrativos inusuales.
- Cuentas, roles o privilegios creados o modificados fuera de las ventanas de mantenimiento.
- Cambios inesperados en políticas de autenticación, autorización, postura, perfiles de endpoint, *network device groups* o integraciones.
- Conexiones de red salientes anómalas desde nodos ISE/ISEPIC.
- Procesos, servicios, tareas programadas, archivos o binarios no autorizados, considerando el posible acceso root.
- Diferencias no esperadas entre la configuración actual y respaldos/configuraciones aprobadas.

Solución

Se debe **aplicar inmediatamente las actualizaciones de Cisco** para CVE-2026-6460 en todos los nodos ISE e ISEPIC. Priorizar nodos de administración, *Policy Administration Nodes* (PAN), nodos expuestos o alcanzables desde VPN, redes de usuarios, sucursales, entornos de terceros y segmentos no confiables.

Se debe **actualizar a la versión mínima corregida de cada rama**: 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7 o 3.5 Patch 4. Para ramas fuera de soporte, migrar a una release soportada que incluya el fix.

A continuación compartimos enlaces de ayuda para el proceso de actualización:

- **Guía oficial de actualización de Cisco ISE (Upgrade Journey):**

[Cisco Identity Services Engine Upgrade Journey](#)

Esta guía centraliza la planificación, compatibilidad, respaldos, actualización de nodos y aplicación de *patches* para ISE.

- **Guía de instalación y mantenimiento de Cisco ISE 3.5:**

- [Cisco ISE Installation Guide, Release 3.5](#)

- Incluye requisitos, tareas de mantenimiento y consideraciones para instalaciones en appliance o máquina virtual.

- **Verificación del historial de actualización/parches:**

- [View installation and upgrade history — Cisco ISE](#)

- Cisco indica utilizar el comando `show version history` desde la CLI de ISE para revisar instalaciones, actualizaciones, desinstalaciones y *patches* aplicados.

- **Advisory oficial para CVE 2026 76460:**

- [Cisco PSIRT — Cisco Identity Services Engine Authentication Bypass Vulnerability](#)

- Incluye las versiones corregidas, instrucciones de *hardening* y los *patches* de seguridad requeridos para remediar la vulnerabilidad.

Información adicional:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
- https://www.cisco.com/c/en/us/td/docs/security/ise/upgrade_guide/b_ise_upgrade_journey.html
- https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/install_guide/b_ise_Installation_Guide_35/g_systemrequirements.html
- https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/install_guide/b_ise_Installation_Guide_35/g_maintenancetasks/t_viewinstallupgradehistory.html