# Boletín de alerta

**Boletín Nro.:** 39
**Fecha de publicación:** 17/04/2026
**Tema:** Alerta 2026 – 39 Múltiples vulnerabilidades críticas en productos Cisco (SSM On□Prem, IMC, EPNM e ISE)
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

| Producto | Versiones afectadas |
|---|---|
| Cisco Smart Software Manager On□Prem (SSM On□Prem) | 9□202502, 9□202504, 9□202507, 9□202510 (en general 9□202502 a 9□202510, asociadas a CVE□2026□20160/20093/20094) nvd.nist+3 |
| Cisco Identity Services Engine (ISE) 3.1 | 3.1.0 y 3.1.0 Patch 1–10 nvd.nist+2 |
| Cisco Identity Services Engine (ISE) 3.2 | 3.2.0 y Patches 1–7 nvd.nist+2 |
| Cisco Identity Services Engine (ISE) 3.3 | 3.3.0 y Patches 1–7 nvd.nist+2 |
| Cisco Identity Services Engine (ISE) 3.4 | 3.4.0 y Patches 1–3 nvd.nist+2 |
| Cisco Identity Services Engine (ISE) 3.5 | No vulnerable (incluida como rama fija de referencia) |

## Descripción

Se han publicado varias vulnerabilidades críticas en productos Cisco, incluyendo Cisco Smart Software Manager On□Prem (SSM On□Prem) e Identity Services Engine (ISE), con CVEs destacados como **CVE□2026□20160** y **CVE□2026□20093** (SSM On□Prem, CVSS 9.8, RCE no autenticada y bypass de autenticación) y **CVE□2026□20186** y **CVE□2026□20180** (Cisco ISE, CVSS 10.0 y 9.9–10.0, inyección de comandos desde cuentas Read□Only Admin). Su explotación puede dar a atacantes remotos control casi completo de los appliances afectados, permitir la manipulación de credenciales y políticas, y causar denegaciones de servicio en componentes críticos de gestión y control de acceso de la red.

Se detalle de las vulnerabilidades que afecta a Cisco SSM On□Prem / IMC / EPNM

- **CVE-2026-20160 – Cisco Smart Software Manager On-Prem – CVSS 9.8 (Crítica)**

Se describe como una vulnerabilidad crítica en **Cisco Smart Software Manager On-Prem** que expone involuntariamente un servicio interno. Un atacante remoto no autenticado puede acceder a ese servicio y enviar peticiones manipuladas hacia la API interna del sistema, lo que permite ejecutar **comandos arbitrarios** en el sistema operativo con privilegios elevados (equivalentes a administrador del appliance). El impacto incluye compromiso completo del servidor de licenciamiento SSM On-Prem y la posibilidad de manipular registros de licencias y configuraciones asociadas.

- **CVE-2026-20093 – Cisco Smart Software Manager On-Prem – CVSS 9.8 (Crítica)**

**CVE-2026-20093** afecta también a Cisco SSM On-Prem y se debe a **validación insuficiente de entrada** en la funcionalidad de cambio de contraseña. Un atacante remoto no autenticado puede explotar esta falla para **omitir la autenticación**, cambiar la contraseña de cualquier usuario (incluido administrador) y, a continuación, iniciar sesión con privilegios completos. Esto permite el control total de la interfaz de administración de SSM On-Prem sin necesidad de credenciales previas.

- **CVE-2026-20094 – Cisco Smart Software Manager On-Prem – CVSS 8.8 (Alta)**

En **CVE-2026-20094**, la interfaz web de SSM On-Prem presenta un fallo de **inyección de comandos**. En este caso se requiere que el atacante ya disponga de una cuenta autenticada, pero incluso con un rol de **solo lectura** puede construir peticiones HTTP especialmente manipuladas para que el sistema ejecute comandos en el sistema operativo como usuario **root**. Aunque exige autenticación, la combinación con robo de credenciales o explotación de CVE-2026-20093 aumenta significativamente el riesgo de compromiso

Y a continuación se detallan las vulnerabilidades del producto Cisco Identity Services Engine – ISE:

- **CVE-2026-20186 – Cisco Identity Services Engine (ISE) – CVSS 10.0 (Crítica)**

CVE-2026-20186 es una vulnerabilidad de inyección de comandos en Cisco Identity Services Engine (ISE) causada por una validación insuficiente de datos proporcionados por el usuario en ciertas peticiones HTTP hacia la interfaz de administración. Un atacante remoto autenticado con una cuenta de al menos Read-Only Admin puede enviar solicitudes manipuladas para conseguir que el sistema ejecute comandos en el sistema operativo subyacente. La explotación exitosa permite obtener shell en el appliance y elevar privilegios hasta root, comprometiendo plenamente el nodo ISE y pudiendo provocar denegación de servicio si se trata de un despliegue de nodo único (afectando la autenticación de nuevos endpoints en la red).

- **CVE-2026-20180 – Cisco Identity Services Engine (ISE) – CVSS 9.9–10.0 (Crítica)**

CVE-2026-20180 es una vulnerabilidad muy similar a la anterior, donde el procesamiento de determinadas peticiones HTTP por parte de la interfaz de administración permite inyección de comandos en el sistema operativo cuando el atacante dispone de credenciales de Read-Only Admin. Del mismo modo, puede derivar en ejecución de comandos con privilegios elevados, escalada a root y potencial compromiso casi total del dispositivo ISE. Diversas fuentes señalan que encadenar CVE-2026-20180 y CVE-2026-20186 es un

escenario de ataque muy creíble para estabilizar acceso persistente y obtener control completo sobre el servidor de políticas NAC

En el caso de Cisco SSM On‑Prem, estas vulnerabilidades permiten a atacantes remotos —incluso sin credenciales— tomar control del servidor de licencias, alterar credenciales de administración y ejecutar comandos como root. Dado que SSM On‑Prem suele estar vinculado a la gestión de licencias de múltiples equipos Cisco, su compromiso puede facilitar manipulaciones de configuración y uso de la infraestructura para movimiento lateral.

Con relación a Cisco ISE, que se encuentra en el núcleo de las arquitecturas de control de acceso a la red (NAC), un atacante que explote CVE‑2026‑20180/20186 puede convertir una simple cuenta de sólo lectura en acceso root al appliance, modificar políticas de autenticación/autorización, desplegar puertas traseras y provocar interrupciones en el servicio de autenticación de usuarios y dispositivos

## Solución:

- **En Cisco SSM On‑Prem / IMC / EPNM, se recomienda** Aplicar las actualizaciones recomendadas por Cisco que corrigen **CVE‑2026‑20160, CVE‑2026‑20093, CVE‑2026‑20094**. También se recomienda restringir el acceso a la interfaz de administración de SSM On‑Prem a redes de gestión dedicadas y reforzar autenticación para cuentas administrativas.
    - *Para la guía de actualización propiamente dicha, Cisco indica usar el procedimiento estándar de upgrade de SSM On?Prem desde la GUI y actualizar directamente a la release recomendada en el advisory; no hay un documento separado específico para estas CVE.*

- **En Cisco Identity Services Engine (ISE)** Actualizar Cisco ISE a las versiones corregidas publicadas en el advisory oficial de Cisco sobre **Remote Code Execution Vulnerabilities in Cisco ISE** (para ramas 3.1, 3.2, 3.3 y 3.4).
    - Limitar el acceso a la consola de administración de ISE a **jump hosts** o segmentos de gestión; revisar periódicamente permisos de perfiles Read‑Only Admin.
    - Auditar logs de administración en busca de actividad anómala (inicios de sesión inusuales, cambios de configuración inesperados) que puedan indicar intentos de explotación.
    - A continuación se comparta un enlance de ayuda generico de productos ISE: https://software.cisco.com/download/home/283802664/type/282046477

| Producto | Versión recomendada / segura |
|---|---|
| Cisco Smart Software Manager On‑Prem (SSM On‑Prem) | 9‑202601 o superior ccb.belgium+2 |
| Cisco Identity Services Engine (ISE) 3.1 | Migrar a rama corregida (3.2 P8, 3.3 P8, 3.4 P4 o 3.5) thehackernews+1 |
| Cisco Identity Services Engine (ISE) 3.2 | 3.2 Patch 8 o superior thehackernews+1 |
| Cisco Identity Services Engine (ISE) 3.3 | 3.3 Patch 8 o superior thehackernews+1 |
| Cisco Identity Services Engine (ISE) 3.4 | 3.4 Patch 4 o superior thehackernews+1 |
| Cisco Identity Services Engine (ISE) 3.5 | 3.5 (o posteriores soportadas) thehackernews+1 |

# Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr
- https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-cssm-priv-esc-xRAnOuO8.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8
- https://www.runzero.com/blog/cisco-ssm-on-prem/
- https://ccb.belgium.be/advisories/warning-remote-code-execution-vulnerabilities-multiple-cisco-products-patch-immediately
- https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-030/
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv
- https://software.cisco.com/download/home/283802664/type/282046477
- https://www.tenable.com/plugins/nessus/306554
- https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html