I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad Crítica de Software / Gestión de Servidores.
Tipo de Incidente: Ejecución remota de código / Evasión de autenticación.
Nivel de riesgo: Alta.

II. ALERTA

Figura 1. Fallas críticas en Cisco IMC y SSM On-Prem (CVE-2026-20093 y CVE-2026-20160) - figura referencial

Las recientes alertas de seguridad relacionadas con productos Cisco han identificado dos vulnerabilidades críticas: CVE-2026-20093 falla de manejo incorrecto de cambio de contraseña en Cisco Integrated Management Controller (Cisco IMC) y CVE-2026-20160 origina exposición accidental de servicio interno accesible desde la API de Cisco Smart Software Manager On-Prem. Ambas fallas presentan un alto nivel de riesgo, ya que su explotación podría permitir a un atacante remoto no autenticado, envíe solicitudes manipuladas logrando ejecutar comandos arbitrarios para escalar privilegios elevados incluso a nivel root y omitir la autenticación, cambiar credenciales y obtener acceso administrativo al sistema respectivamente.

III. INTRODUCCIÓN

CVE-2026-20093:

Es una vulnerabilidad de tipo Evasión de Autenticación en Cisco Integrated Management Controller (IMC) que se origina por un manejo incorrecto de las solicitudes de cambio de contraseña enviadas al sistema. Como resultado, un atacante remoto no autenticado puede evadir los mecanismos de autenticación y obtener acceso completo al sistema como administrador.

Como consecuencia, esta vulnerabilidad permite a un atacante ejecutar acciones con privilegios equiparables a los de un administrador, como la modificación de credenciales de usuarios, la creación de nuevas cuentas administrativas, establecer mecanismos de persistencia sin generar alertas y controlar parámetros críticos de configuración en los dispositivos afectados.

CVE-2026-20160:

Es una vulnerabilidad de tipo Ejecución Remota de Código (RCE) en Cisco Smart Software Manager On-Prem que se origina por la exposición de un servicio interno a través de su API, sin validación adecuada de las solicitudes entrantes. Como resultado, un atacante remoto puede enviar solicitudes manipuladas para ejecutar comandos arbitrarios en el sistema con privilegios elevados, incluso a nivel root.

Como consecuencia, esta vulnerabilidad permite a un atacante ejecutar acciones críticas con privilegios de administrador, como ejecución de comandos arbitrarios, compromiso completo del servidor, persistencia en el sistema y movimiento lateral dentro de la red, afectando la confidencialidad, integridad y disponibilidad de los activos de la organización.

IV. VECTOR DE ATAQUE

CVE-2026-20093, esta vulnerabilidad en Cisco Integrated Management Controller posee una severidad CRITICAL con una puntación CVSS: 3.1 de 9.8 tipo /AV: N /AC: L /PR: N /UI: N /S: U /C: H /I: H /A: H.

CVE-2026-20160, esta vulnerabilidad en Cisco Smart Software Manager On-Prem posee una severidad CRITICAL con una puntación CVSS: 3.1 de 9.8 tipo /AV: N /AC: L /PR: N /UI: N /S: U /C: H /I: H /A: H.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Fabricante	Producto	Componente	CVE	Versión afectada
Cisco	5000 Series Enterprise Network Compute Systems (ENCS)	Cisco IMC vulnerable releases	CVE-2026-20093	Versiones vulnerables del software IMC
Cisco	Catalyst 8300 Series Edge uCPE	Cisco IMC vulnerable releases	CVE-2026-20093	Versiones vulnerables del software IMC
Cisco	UCS C-Series M5 y M6 Rack Servers (modo independiente)	Cisco IMC vulnerable releases	CVE-2026-20093	Versiones vulnerables del software IMC
Cisco	UCS E-Series Servers M3 y M6	Cisco IMC vulnerable releases	CVE-2026-20093	Versiones vulnerables del software IMC
Cisco	APIC Servers, Catalyst Center, Secure Firewall Management Center, Secure Network Analytics Appliances	Cisco IMC UI expuesta en appliances preconfigurados con UCS C-Series Servers afectados	CVE-2026-20093	Versiones vulnerables del software IMC
Cisco	Smart Software Manager On-Prem	API/CLI del servicio SSM On-Prem	CVE-2026-20160	Versiones vulnerables según Cisco Security Advisory
Cisco	Appliances gestionados por SSM On-Prem	Servicio interno expuesto	CVE-2026-20160	Versiones vulnerables según Cisco Security Advisory

***Tabla 1**.Productos y* Versiones Afectadas - Fallas críticas en Cisco IMC y SSM On-Prem (CVE-2026-20093 y CVE-2026-20160)

VI. INDICADORES DE COMPROMISO.

Dado que **CVE-2026-20093**, Cisco Integrated Management Controller (IMC) es el controlador de gestión de zócalo (BMC) integrado en los servidores Cisco UCS y C-Series. Las interfaces BMC son objetivos de muy alto valor porque operan por debajo del nivel del sistema operativo. Un atacante que compromete a IMC tiene acceso a:

- Control completo a nivel de hardware del servidor.
- Acceso a la consola KVM virtual (teclado, video, ratón): equivalente a sentarse frente a la máquina.
- Capacidad para montar medios virtuales y arrancar desde imágenes controladas por atacantes.
- Capacidades de modificación del BIOS y del firmware.
- Configuración de la interfaz de red, incluyendo la capacidad de interceptar o redirigir el tráfico.
- Acceso persistente que sobrevive a la reinstalación del sistema operativo.
- Una omisión de autenticación CVSS 9.8 en esta interfaz significa que un atacante que puede llegar al puerto de red IMC puede tomar el control completo del servidor sin ninguna credencial.
- Solicitudes HTTP POST malintencionadas.

CVE-2026-20160, cualquier envió de solicitud malintencionada especialmente diseñada a la API de Cisco Smart Software Manager On-Prem (SSM On-Prem), donde el atacante con un exploit correcto puede activar ejecución de comandos en el SO.

VII. RECOMENDACIONES:

- Aplicar los parches de seguridad proporcionados por Cisco.
- Restringir el acceso a las interfaces IMC y SSM On-Prem mediante segmentación de red.
- Implementar controles de acceso basados en IP.
- Monitorear logs de cambios de contraseña y accesos administrativos sospechosos.
- Deshabilitar la exposición directa de IMC y SSM On-Prem a Internet.
- Integrar soluciones EDR/XDR y correlación de eventos en SIEM.
- Realizar auditorías de cuentas privilegiadas y rotación de credenciales.

- Implementar autenticación multifactor (MFA) en cuentas administrativas.
- Ejecutar pruebas de vulnerabilidad y pentesting centradas en las interfaces de gestión.
- Limitar privilegios administrativos al mínimo necesario.
- Capacitar al personal de TI sobre explotación de vulnerabilidades y buenas prácticas de seguridad.

VIII. DESCARGO DE RESPONSABILIDAD.

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

INCIBE-CERT (2026). Múltiples vulnerabilidades en productos de CISCO. https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-10

INCIBE-CERT (2026). Vulnerabilidad CVE-2026-20160 en Cisco Smart Software Manager On-Prem. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/CVE-2026-20160

INCIBE-CERT (2026). Vulnerabilidad CVE-2026-20093 en Cisco IMC. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/CVE-2026-20093

CIBERSAFETY (2026). CVE-2026-20160 y CVE-2026-20093 en Cisco: vulnerabilidades críticas. https://cibersafety.com/cve-2026-20160-cve-2026-20093-cisco/

CSIRT TELCONET (2026). Vulnerabilidad crítica en Cisco Smart Software Manager On-Prem permite ejecución remota de comandos. https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-cisco-smart-software-manager-on-prem-permite-ejecucion-remota-de-comandos/

CSIRT TELCONET (2026). Vulnerabilidad crítica en Cisco IMC permite omitir autenticación. https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-cisco-imc-permite-omitir-autenticacion/