Cisco ha publicado actualizaciones para corregir una vulnerabilidad crítica de seguridad en el Integrated Management Controller (IMC), la cual, si es explotada con éxito, podría permitir a un atacante remoto sin autenticación eludir los mecanismos de acceso y obtener control del sistema con privilegios elevados.

La falla, identificada como CVE-2026-20093, posee una puntuación CVSS de 9.8 sobre un máximo de 10.0.

"Esta vulnerabilidad se debe a un manejo incorrecto de las solicitudes de cambio de contraseña", indicó Cisco en un aviso emitido el miércoles. *"Un atacante podría aprovechar esta falla enviando una solicitud HTTP especialmente manipulada a un dispositivo afectado."*

"Si la explotación tiene éxito, el atacante podría evadir la autenticación, modificar las contraseñas de cualquier usuario del sistema, incluyendo cuentas de administrador, y acceder al sistema con dichos privilegios."

El investigador de seguridad «jyh» fue reconocido por descubrir y reportar esta vulnerabilidad. El problema afecta a los siguientes productos, independientemente de su configuración:

- 5000 Series Enterprise Network Compute Systems (ENCS) – Corregido en la versión 4.15.5
- Catalyst 8300 Series Edge uCPE – Corregido en la versión 4.18.3
- UCS C-Series M5 y M6 Rack Servers en modo independiente – Corregido en las versiones 4.3(2.260007), 4.3(6.260017) y 6.0(1.250174)
- UCS E-Series Servers M3 – Corregido en la versión 3.2.17
- UCS E-Series Servers M6 – Corregido en la versión 4.15.3

Otra vulnerabilidad crítica solucionada por Cisco afecta a Smart Software Manager On-Prem (SSM On-Prem), la cual podría permitir a un atacante remoto sin autenticación ejecutar comandos arbitrarios en el sistema operativo subyacente. Esta falla, registrada como CVE-2026-20160 (CVSS 9.8), se origina por la exposición inadvertida de un servicio interno.

“Un atacante podría explotar esta vulnerabilidad enviando una solicitud manipulada a la API del servicio expuesto”, explicó Cisco. *“Una explotación exitosa permitiría ejecutar comandos en el sistema operativo con privilegios de nivel root.”*

Las correcciones para este problema fueron incluidas en la versión 9-202601 de Cisco SSM On-Prem. Cisco señaló que la vulnerabilidad fue detectada internamente durante la resolución de un caso de soporte del Cisco Technical Assistance Center (TAC).

Aunque ninguna de estas vulnerabilidades ha sido explotada activamente hasta el momento, diversas fallas de seguridad recientemente divulgadas en productos de Cisco han sido utilizadas por actores maliciosos. Dado que no existen soluciones alternativas temporales, se recomienda a los clientes actualizar a las versiones corregidas para garantizar una protección adecuada.