Boletín informativo
Vulnerabilidad en producto de comunicación de Cisco

CSIRTSALUD-AV-20260122-26 **TLP: CLEAR**

Incidente ID:	0026
Fecha del reporte:	22/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en productos de comunicaciones unificadas de Cisco
Herramienta de detección	N/A
Activo involucrado:	Cisco
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad de **zero-day** CVE-2026-20045 que actualmente se encuentra siendo explotada activamente, esta vulnerabilidad afecta los productos Unified CM y Webex de CISCO, que permiten conectar infraestructura local (Unified CM) con servicios en la nube (Webex App).

Esta vulnerabilidad es de nivel alta (CVSS: 8.2), pero Cisco informa que la eleva a nivel Crítica debido a que han encontrado que la están explotando activamente y adicionalmente debido a que la elevación de privilegios puede llegar hasta el nivel root, es una vulnerabilidad de ejecución remota de código que afecta productos de comunicaciones unificadas de Cisco.

Descripción:

La Agencia de Seguridad Cibernética e Infraestructura de EE. UU. (CISA) emitió una alerta urgente tras confirmar la explotación activa de una vulnerabilidad **zero-day** de ejecución remota de código (RCE) la falla afecta a Cisco Unified Communications Manager (Unified CM), Unified CM Session Management Edition (SME), Unified CM IM & Presence, Cisco Unity Connection y Webex Calling Dedicated Instance.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

La falla, registrada como **CVE-2026-20045**, permite ataques de inyección de código con acceso inicial a nivel usuario y escalamiento completo a privilegios root, afectando principalmente sistemas de comunicación empresarial expuestos a internet.

Este problema crítico se debe a una validación de entrada incorrecta en las plataformas de comunicación de Cisco, en consonancia con la norma CWE-94: Control inadecuado de la generación de código . Los atacantes pueden inyectar código malicioso mediante solicitudes de red manipuladas, omitiendo así la autenticación en algunos casos.

Un atacante podría aprovechar esta vulnerabilidad enviando una secuencia de solicitudes HTTP diseñadas a la interfaz de administración basada en la web de un dispositivo afectado. Un ataque exitoso podría permitir al atacante obtener acceso a nivel de usuario al sistema operativo subyacente y, luego, elevar los privilegios al usuario root. Esto otorga al atacante control total sobre el dispositivo, permitiéndole interceptar comunicaciones, exfiltrar datos sensibles, instalar persistencia, o utilizar el dispositivo como pivote para atacar otras partes de la red interna.

Productos afectados:

La vulnerabilidad afecta a los componentes centrales de la suite de colaboración y comunicaciones de Cisco. Los productos confirmados son:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified CM Session Management Edition (SME)
- Cisco Unified CM IM & Presence Service (IM&P)
- Cisco Unity Connection
- Cisco Webex Calling Dedicated Instance

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Versiones Impactadas:

- Release 12.5 (y anteriores)
- Release 14
- Release 15

Modo de explotación y cadena de infección

La vulnerabilidad reside en una validación incorrecta de las entradas proporcionadas por el usuario en la interfaz de gestión basada en web, en donde un atacante remoto y **no autenticado** envía una secuencia de solicitudes HTTP especialmente diseñadas (crafted HTTP requests) a la interfaz de gestión web del dispositivo vulnerable. Al no validarse correctamente la entrada, el sistema procesa estas solicitudes permitiendo la inyección de comandos arbitrarios que son ejecutados por el sistema operativo subyacente.

Este vector permite que cualquier instancia expuesta a internet sea altamente vulnerable. Los atacantes están escaneando activamente sistemas para explotar esta falla

El uso de esta vulnerabilidad suele alinearse con las siguientes tácticas y técnicas de ataque (MITRE ATT&CK Mapping):

- **T1190 (Exploit Public-Facing Application):** El atacante aprovecha la interfaz web expuesta a internet o a la red interna.
- **T1059 (Command and Scripting Interpreter):** Ejecución de comandos arbitrarios tras la inyección exitosa.
- **T1068 (Exploitation for Privilege Escalation):** Movimiento de acceso nivel usuario a nivel
- **T1595 – Reconocimiento activo (escaneo)**: Los atacantes escanean internet buscando instancias vulnerables expuestas.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones de mitigación:

Cisco ha confirmado que **no existen soluciones alternativas (workarounds)** efectivas; la única solución es parchear. Se recomienda encarecidamente la actualización inmediata dada la explotación activa.

- **Para Release 12.5:** No hay parche directo. Se debe **migrar** inmediatamente a una versión con soporte fijo (Release 14 o 15).

- **Para Release 14:**

– Actualizar a **14SU5** (si está disponible) o; Aplicar el parche específico: ciscocm.V14SU4a_CSCwr21851_remote_code_v1.cop.sha512

- **Para Release 15:**

– Actualizar a **15SU4** (planeado para marzo 2026) o; Aplicar los parches actuales:

ciscocm.V15SU2_CSCwr21851_remote_code_v1.cop.sha512
ociscocm.V15SU3_CSCwr21851_remote_code_v1.cop.sha512

-
- **Para Cisco Unity Connection (Ver 14):**

- Aplicar parche: ciscocm.cuc.CSCwr29208_C0266-1.cop.sha512

Se debe tener en cuenta verifica siempre el hash (SHA512) de los archivos .cop antes de la instalación para asegurar su integridad.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- https://thehackernews.com/2026/01/cisco-fixes-actively-exploited-zero-day.html
- https://www.cve.org/CVERecord?id=CVE-2026-20045
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-zero-day-rce-en-productos-cisco-unified-communications/
- https://www.tenable.com/cve/CVE-2026-20045

Para descarga de parches consultar las siguientes páginas:

- https://software.cisco.com/download/home/286331949/type/286319533/release/15SU3
- https://software.cisco.com/download/home/286328409/type/286319533/release/14SU4
- https://software.cisco.com/download/home/286331940/type/286319236/release/15SU3a
- https://software.cisco.com/download/home/286331940/type/286319236/release/15SU2
- https://software.cisco.com/download/home/286328117/type/286319236/release/14SU4a

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570