

Alerta ID:	116
Fecha del reporte:	24/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Explotación activa de vulnerabilidad crítica en Cisco Unified Communications Manager podría permitir compromiso total de sistemas de comunicaciones empresariales
Herramienta de detección	N/A
Activo involucrado:	Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (SME), servidores de comunicaciones IP, plataformas de telefonía corporativa, servicios VoIP, sistemas de atención al usuario, centros de contacto, infraestructura de comunicaciones hospitalarias y plataformas de colaboración empresarial
Tipo de alerta:	Alerta
Nivel de riesgo:	Critico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la explotación activa de la vulnerabilidad crítica CVE-2026-20230 identificada en Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME), plataformas ampliamente utilizadas para la gestión de comunicaciones unificadas, telefonía IP y servicios de colaboración empresarial. Cisco publicó actualizaciones de seguridad para corregir esta vulnerabilidad a comienzos de junio de 2026; sin embargo, recientemente se confirmó que actores maliciosos ya están explotando la falla en escenarios reales.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que esta vulnerabilidad podría generar sobre:



- plataformas de telefonía IP institucional;
- sistemas de atención al usuario;
- centros de contacto hospitalarios;
- plataformas de comunicaciones clínicas;
- infraestructura de colaboración empresarial;
- servicios de voz y video corporativos;
- sistemas de soporte operativo;
- servidores Linux subyacentes;
- entornos administrativos de comunicaciones;
- y activos críticos conectados a la infraestructura de comunicaciones.

En el sector salud, la disponibilidad y seguridad de las plataformas de comunicaciones resulta esencial para soportar procesos asistenciales, coordinación clínica, referencia y contrarreferencia de pacientes, gestión de emergencias y operación administrativa institucional.

Descripción:

Investigadores de seguridad y diversas organizaciones especializadas en inteligencia de amenazas han reportado la explotación activa de la vulnerabilidad CVE-2026-20230, una falla crítica que afecta a Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME), plataformas ampliamente utilizadas para la gestión de comunicaciones unificadas, telefonía IP y servicios de colaboración empresarial en organizaciones públicas y privadas.

La vulnerabilidad se origina en el componente WebDialer, una funcionalidad utilizada para facilitar la integración entre aplicaciones web y servicios de telefonía. Debido a una validación insuficiente de determinadas solicitudes HTTP, un atacante remoto no autenticado puede explotar una condición de tipo Server-Side Request Forgery (SSRF) para inducir al sistema vulnerable a procesar solicitudes no autorizadas. Esta capacidad permite interactuar con recursos internos del servidor y constituye el punto de partida para la ejecución de acciones maliciosas de mayor impacto.



De acuerdo con la información publicada por Cisco, la explotación exitosa de la vulnerabilidad no se limita únicamente a la ejecución de ataques SSRF. Los atacantes también pueden aprovechar la falla para realizar escritura arbitraria de archivos dentro del sistema operativo subyacente, permitiendo la creación o modificación de archivos utilizados posteriormente para facilitar procesos de escalamiento de privilegios. Como consecuencia, un actor malicioso podría obtener acceso de nivel root, comprometiendo completamente la plataforma afectada y adquiriendo control total sobre los servicios de comunicaciones administrados por el servidor.

La situación reviste especial preocupación debido a que investigadores de seguridad han confirmado la disponibilidad pública de herramientas y pruebas de concepto (PoC) que simplifican significativamente la explotación de la vulnerabilidad. Asimismo, se ha evidenciado actividad maliciosa dirigida contra sistemas expuestos a Internet, lo que indica que actores de amenaza ya se encuentran intentando comprometer organizaciones que aún no han aplicado las actualizaciones de seguridad publicadas por el fabricante.

Cisco Unified CM constituye el núcleo de la infraestructura de comunicaciones en numerosas organizaciones, centralizando servicios de telefonía IP, comunicaciones internas, centros de contacto, videoconferencia y otros mecanismos de colaboración empresarial. Debido a su rol estratégico, un compromiso exitoso podría permitir a los atacantes afectar la disponibilidad de los servicios de comunicación, alterar configuraciones críticas, acceder a información sensible relacionada con usuarios y dispositivos, crear cuentas privilegiadas, establecer mecanismos de persistencia y utilizar la plataforma comprometida como punto de acceso hacia otros activos tecnológicos de la organización.

En el contexto del sector salud, la explotación de esta vulnerabilidad podría impactar directamente plataformas utilizadas para soportar procesos asistenciales, coordinación clínica, gestión de emergencias, telemedicina, atención de usuarios, servicios administrativos hospitalarios y comunicaciones entre profesionales de la salud. La afectación de estos servicios podría generar interrupciones operativas significativas, comprometer la continuidad de la atención y aumentar el riesgo de incidentes que involucren información sensible de pacientes y procesos críticos institucionales.



Consecuencias de la explotación



La explotación exitosa de esta vulnerabilidad podría generar impactos severos sobre la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica institucional.

Uno de los principales riesgos corresponde al compromiso total de los servidores Cisco Unified CM mediante la obtención de privilegios de nivel root. Una vez alcanzado este nivel de acceso, un atacante podría controlar completamente la plataforma afectada y realizar modificaciones no autorizadas sobre los servicios de comunicaciones institucionales.

En escenarios de explotación exitosa, un atacante podría:

- obtener acceso privilegiado al sistema operativo;
- modificar configuraciones críticas de comunicaciones;
- interceptar información relacionada con llamadas;
- alterar servicios de telefonía IP;
- crear cuentas administrativas;
- establecer mecanismos de persistencia;
- comprometer credenciales institucionales;
- y utilizar la plataforma comprometida como punto de entrada hacia otros sistemas corporativos.

La explotación también podría afectar la continuidad operacional de las organizaciones al generar interrupciones en servicios de comunicación críticos utilizados para la coordinación de actividades asistenciales y administrativas.

En el sector salud, una afectación sobre las plataformas de comunicaciones podría impactar directamente procesos relacionados con atención de pacientes, coordinación clínica, telemedicina, gestión de emergencias y servicios administrativos hospitalarios.



Modo de explotación del ataque



Fase 1 – Identificación de objetivos potenciales

El proceso de explotación inicia cuando los actores de amenaza identifican organizaciones que utilizan Cisco Unified Communications Manager (Unified CM) o Unified CM Session Management Edition (SME) para la gestión de sus servicios de telefonía IP y comunicaciones empresariales. Debido a que estas plataformas suelen encontrarse expuestas parcial o totalmente a redes corporativas e incluso a Internet para soportar funcionalidades de administración remota, integración con aplicaciones externas y servicios de colaboración, representan objetivos de alto valor para los atacantes.

Durante esta fase, los actores maliciosos realizan actividades de reconocimiento orientadas a identificar sistemas potencialmente vulnerables mediante técnicas de inteligencia de fuentes abiertas (OSINT), análisis de infraestructura expuesta, motores de búsqueda especializados, certificados digitales públicos, escaneo de servicios y recopilación de información publicada por las organizaciones objetivo.

Las actividades realizadas durante esta etapa pueden incluir:

- identificación de organizaciones que utilizan Cisco Unified CM;
- descubrimiento de servidores expuestos a Internet;
- identificación de servicios WebDialer accesibles;
- recopilación de información sobre la infraestructura tecnológica;
- identificación de entidades del sector salud;
- análisis de tecnologías asociadas;
- y detección de posibles versiones vulnerables.

El objetivo principal consiste en localizar plataformas susceptibles de explotación que permitan obtener acceso a sistemas de comunicaciones críticos o facilitar el compromiso de otros activos institucionales.



Fase 2 – Reconocimiento y análisis de la plataforma

Una vez identificado el objetivo, los actores de amenaza realizan actividades de reconocimiento más detalladas para comprender la arquitectura de la plataforma y validar las condiciones necesarias para la explotación de la vulnerabilidad.

Durante esta etapa, los atacantes intentan determinar la versión exacta del software instalada, verificar si el servicio WebDialer se encuentra habilitado, identificar configuraciones de seguridad implementadas y comprender las relaciones existentes entre el servidor de comunicaciones y otros componentes de la infraestructura.

Asimismo, los actores maliciosos buscan identificar mecanismos de autenticación, interfaces administrativas, sistemas asociados y recursos internos que podrían ser accesibles mediante la explotación de la vulnerabilidad SSRF.

- Las actividades realizadas durante esta fase pueden incluir:
- identificación de versiones instaladas;
- validación de componentes vulnerables;
- análisis de interfaces web disponibles;
- identificación de servicios internos accesibles;
- reconocimiento de mecanismos de autenticación;
- análisis de configuraciones de seguridad;
- y evaluación de posibles rutas de explotación.

El objetivo consiste en determinar la viabilidad del ataque y seleccionar la estrategia más adecuada para comprometer el sistema.

Fase 3 – Preparación del vector de ataque

Posteriormente, los actores de amenaza preparan los recursos necesarios para explotar la vulnerabilidad identificada. Dependiendo del nivel de acceso requerido y de las características específicas del entorno objetivo, los atacantes desarrollan solicitudes HTTP especialmente diseñadas para interactuar con el componente vulnerable.



Durante esta fase se preparan cargas útiles orientadas a aprovechar la condición SSRF y a manipular el comportamiento del servidor para generar solicitudes internas no autorizadas. Asimismo, pueden desarrollarse mecanismos destinados a facilitar la creación de archivos arbitrarios y preparar el posterior escalamiento de privilegios.

Las actividades observadas durante esta etapa pueden incluir:

- desarrollo de solicitudes maliciosas;
- preparación de cargas de explotación;
- validación de rutas accesibles internamente;
- pruebas de interacción con servicios internos;
- preparación de archivos destinados al escalamiento de privilegios;
- configuración de infraestructura de soporte;
- y generación de mecanismos de persistencia.

El objetivo consiste en disponer de todos los elementos necesarios para ejecutar la explotación de manera exitosa y minimizar las posibilidades de detección.

Fase 4 – Explotación de la vulnerabilidad

Una vez preparado el entorno de ataque, los actores maliciosos envían solicitudes especialmente diseñadas al servicio vulnerable. Como resultado, el servidor procesa peticiones que no deberían ser permitidas, posibilitando la interacción con recursos internos y la ejecución de acciones fuera de los controles normales de seguridad.

La explotación inicial aprovecha la vulnerabilidad SSRF para acceder a componentes internos del sistema y manipular determinados procesos que posteriormente permiten la creación o modificación de archivos dentro del sistema operativo subyacente.



Dependiendo de la configuración afectada, esta fase puede ejecutarse de forma remota sin requerir autenticación previa, lo que incrementa significativamente el nivel de riesgo asociado a la vulnerabilidad.

Las actividades desarrolladas durante esta etapa pueden orientarse a:

- explotar la vulnerabilidad SSRF;
- interactuar con recursos internos protegidos;
- evadir controles de acceso;
- manipular solicitudes procesadas por el servidor;
- acceder a funcionalidades restringidas;
- preparar la escritura de archivos arbitrarios;
- y obtener acceso inicial al entorno afectado.

El objetivo consiste en establecer una posición inicial dentro de la plataforma vulnerable que permita continuar con las fases posteriores del ataque.

Fase 5 – Escritura arbitraria de archivos

Tras la explotación inicial, los atacantes aprovechan las capacidades obtenidas para crear, modificar o sobrescribir archivos dentro del sistema operativo que soporta Cisco Unified CM.

La escritura arbitraria de archivos constituye una de las etapas más críticas del ataque, ya que permite introducir componentes maliciosos, alterar configuraciones del sistema o preparar mecanismos destinados a elevar privilegios y garantizar la persistencia del acceso obtenido.

Dependiendo del alcance alcanzado por el atacante, podrían realizarse actividades relacionadas con:

- creación de archivos maliciosos;
- modificación de configuraciones críticas;



- instalación de componentes de persistencia;
- alteración de archivos del sistema;
- preparación de mecanismos de escalamiento;
- modificación de procesos internos;
- y habilitación de accesos no autorizados.

El objetivo consiste en preparar las condiciones necesarias para comprometer completamente el sistema operativo.

Fase 6 – Escalamiento de privilegios

Una vez que los archivos han sido creados o modificados, los actores de amenaza aprovechan dichos cambios para elevar privilegios hasta obtener acceso de nivel root sobre el servidor afectado.

La obtención de privilegios elevados permite evadir controles de seguridad, modificar configuraciones sensibles y ejecutar acciones administrativas con el máximo nivel de autorización disponible dentro del sistema operativo.

Las actividades observadas durante esta etapa pueden incluir:

- elevación de privilegios;
- ejecución de comandos administrativos;
- modificación de configuraciones de seguridad;
- creación de usuarios privilegiados;
- instalación de herramientas de administración remota;
- establecimiento de persistencia;
- y consolidación del acceso obtenido.

El objetivo consiste en obtener control total sobre la plataforma comprometida.



Fase 7 – Movimiento lateral y expansión del compromiso

Finalmente, una vez comprometido el servidor Cisco Unified CM, los atacantes pueden utilizar el acceso obtenido para ampliar el alcance del incidente hacia otros activos tecnológicos de la organización.

Debido a que estas plataformas suelen mantener comunicación con múltiples sistemas corporativos, directorios de usuarios, plataformas de autenticación, servicios de colaboración y componentes de infraestructura, un compromiso exitoso puede facilitar actividades de movimiento lateral y expansión del ataque.

Las actividades realizadas habitualmente durante esta fase incluyen:

- reconocimiento interno de la infraestructura;
- identificación de servidores críticos;
- descubrimiento de servicios corporativos;
- búsqueda de credenciales adicionales;
- acceso a sistemas conectados;
- exfiltración de información sensible;
- despliegue de malware;
- y establecimiento de mecanismos permanentes de acceso.

En el sector salud, esta fase podría permitir que los atacantes alcancen plataformas de gestión hospitalaria, sistemas clínicos, servicios de directorio activo, aplicaciones administrativas y otros activos críticos que soportan la prestación de servicios de salud, incrementando significativamente el impacto potencial del incidente.



Vulnerabilidades asociadas



Server-Side Request Forgery (SSRF)

- **Descripción:** La vulnerabilidad principal identificada en CVE-2026-20230 corresponde a una falla de tipo Server-Side Request Forgery (SSRF) que afecta el servicio WebDialer de Cisco Unified CM. Esta debilidad permite que un atacante remoto y no autenticado envíe solicitudes HTTP especialmente manipuladas para que el servidor procese peticiones no autorizadas hacia recursos internos o externos.
- **Impacto:** La explotación exitosa puede permitir la interacción con recursos internos protegidos, facilitar la escritura arbitraria de archivos y constituir la base para posteriores actividades de compromiso del sistema. En determinados escenarios puede derivar en el control completo de la plataforma afectada.

Escritura arbitraria de archivos

- **Descripción:** Como consecuencia de la explotación de la vulnerabilidad SSRF, un atacante podría crear o sobrescribir archivos dentro del sistema operativo subyacente. Esta capacidad permite modificar componentes críticos y preparar mecanismos para la ejecución de acciones maliciosas adicionales.
- **Impacto:** La escritura arbitraria de archivos puede facilitar la instalación de componentes maliciosos, la alteración de configuraciones del sistema y la preparación de mecanismos destinados al escalamiento de privilegios.



Escalamiento de privilegios a nivel Root

- **Descripción:** La vulnerabilidad permite que los archivos creados durante la explotación sean utilizados para elevar privilegios hasta alcanzar acceso root sobre el sistema operativo que soporta la plataforma Cisco Unified CM.
- **Impacto:** El acceso root proporciona control total sobre el servidor comprometido, permitiendo la modificación de configuraciones, instalación de software malicioso, creación de usuarios privilegiados, exfiltración de información y afectación de servicios críticos institucionales.

Recomendaciones



Identificar de manera inmediata las instancias vulnerables

Las organizaciones deben realizar un inventario completo de los servidores Cisco Unified Communications Manager (Unified CM) y Unified CM SME desplegados dentro de su infraestructura tecnológica. Se recomienda verificar versiones instaladas, componentes habilitados y dependencias asociadas para determinar el nivel de exposición existente frente a la vulnerabilidad CVE-2026-20230.

Aplicar las actualizaciones de seguridad publicadas por Cisco

Cisco ha publicado actualizaciones destinadas a corregir la vulnerabilidad identificada. Las entidades deben priorizar la aplicación de los parches de seguridad en todos los sistemas afectados, especialmente aquellos expuestos a redes externas o utilizados para soportar procesos críticos de la organización. Antes de implementar las actualizaciones se recomienda realizar respaldos completos y validar procedimientos de recuperación ante posibles contingencias.



Revisar y restringir el uso del servicio WebDialer

Dado que la vulnerabilidad se encuentra asociada al componente WebDialer, las organizaciones deben verificar si este servicio se encuentra habilitado y evaluar su necesidad operativa. En aquellos casos donde no sea indispensable para la operación institucional, se recomienda deshabilitarlo temporalmente hasta completar el proceso de actualización y validación de seguridad.

Limitar la exposición de interfaces administrativas

Las interfaces de administración de Cisco Unified CM no deben encontrarse accesibles directamente desde Internet. Se recomienda implementar controles de segmentación de red, listas de control de acceso (ACL), VPN corporativas y mecanismos de acceso seguro que permitan restringir la administración únicamente a personal autorizado y desde segmentos controlados de la infraestructura.

Fortalecer los mecanismos de autenticación y acceso privilegiado

Las entidades deben revisar los privilegios asignados a usuarios administrativos, aplicar el principio de mínimo privilegio e implementar mecanismos de autenticación multifactor (MFA) cuando sea posible. Asimismo, se recomienda eliminar cuentas obsoletas, revisar accesos compartidos y validar periódicamente la vigencia de los privilegios otorgados.

Monitorear actividades sospechosas y eventos de seguridad

Es recomendable fortalecer el monitoreo de registros relacionados con Cisco Unified CM, prestando especial atención a intentos de acceso no autorizados, creación de usuarios administrativos, modificaciones de configuraciones, generación de archivos inusuales y actividades que puedan indicar explotación de vulnerabilidades o compromiso de cuentas privilegiadas.



Realizar búsquedas proactivas de indicadores de compromiso

Los equipos de seguridad deben ejecutar actividades de threat hunting orientadas a identificar evidencia de explotación previa de la vulnerabilidad. Esto incluye la revisión de archivos recientemente creados o modificados, cambios no autorizados en configuraciones, ejecución de comandos anómalos, conexiones sospechosas y cualquier actividad que pueda indicar la obtención de privilegios elevados dentro del sistema.

Implementar segmentación y controles de movimiento lateral

Se recomienda aislar los servidores de comunicaciones de otros segmentos críticos de la infraestructura mediante controles de segmentación de red. Esta medida contribuye a reducir el impacto potencial de un compromiso, limitando la capacidad de los atacantes para desplazarse hacia sistemas clínicos, administrativos o de almacenamiento de información sensible.

Revisar la integración con servicios corporativos

Las organizaciones deben evaluar las conexiones existentes entre Cisco Unified CM y otros servicios institucionales, tales como Directorio Activo, plataformas de autenticación, sistemas de correo electrónico y aplicaciones corporativas. La revisión de estas integraciones permite identificar posibles rutas de propagación que podrían ser aprovechadas por un atacante en caso de compromiso de la plataforma.

Verificar la integridad de las configuraciones y respaldos

Se recomienda validar periódicamente la integridad de las configuraciones de Cisco Unified CM y mantener copias de seguridad actualizadas y verificadas. Los respaldos deben almacenarse



de forma segura y probarse regularmente para garantizar la capacidad de recuperación ante incidentes de seguridad que afecten la disponibilidad o integridad de la plataforma.

Fortalecer los procesos de gestión de vulnerabilidades

Las entidades deben incorporar esta vulnerabilidad dentro de sus procesos formales de gestión de vulnerabilidades, asegurando la identificación oportuna de activos afectados, la priorización basada en riesgo, la aplicación de controles correctivos y el seguimiento continuo del estado de remediación hasta su cierre definitivo.

Sensibilizar a los equipos técnicos y de operación

Es recomendable informar a los administradores de infraestructura, comunicaciones y seguridad sobre las características de la vulnerabilidad, los mecanismos de explotación observados y los procedimientos de respuesta definidos por la organización. Una adecuada concienciación facilita la detección temprana de actividades sospechosas y reduce los tiempos de respuesta ante posibles incidentes.

Conclusiones

La vulnerabilidad CVE-2026-20230 representa una amenaza crítica para las organizaciones que utilizan Cisco Unified Communications Manager debido a la combinación de explotación remota sin autenticación, disponibilidad pública de código PoC y evidencia de explotación activa en entornos reales.

La capacidad de realizar ataques SSRF, escribir archivos arbitrarios y escalar privilegios hasta nivel root puede conducir al compromiso total de las plataformas de comunicaciones institucionales, afectando servicios esenciales para la operación de las organizaciones.



En el sector salud, donde las comunicaciones desempeñan un papel fundamental en la coordinación clínica y administrativa, resulta prioritario identificar sistemas vulnerables, aplicar las actualizaciones publicadas por Cisco y fortalecer los mecanismos de monitoreo y protección asociados a estas plataformas.

Fuentes:

- <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-cucm-ssrf-cXPnHcW.html>
- <https://www.securityweek.com/hackers-exploiting-cisco-unified-cm-vulnerability>
- <https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-067>
- <https://digital.nhs.uk/cyber-alerts/2026/cc-4791>
- <https://www.sentinelone.com/vulnerability-database/cve-2026-20230>
- <https://www.redlegg.com/blog/security-bulletin-server-side-request-forgery-vulnerability-in-cisco-unified-communications-manager>

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

