| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2026-003 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>ALERTAS DE SEGURIDAD | ecucert<br>V 1.1 |
| TLP: | TLP:CLEAR | | |
| Fecha: | 22-ene-2026 | **CISCO - Vulnerabilidad de ejecución remota. CVE-2026-20045** | Pág.: **1** of **3** |

## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad

**Tipo de incidente:** Información

**Nivel de riesgo:** Alto

## II. ALERTA

Cisco parcheó una falla crítica de ejecución remota de código de día cero, identificada como CVE-2026-20045 (puntaje CVSS de 8,2), explotada activamente en ataques. Un atacante remoto no autenticado puede aprovechar la falla para ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.


**Figura 1.-** *Ilustración asociada a Cisco* ***Fuente: The hacker news***

## III. INTRODUCCIÓN

Se ha identificado una vulnerabilidad crítica en Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unity Connection y Cisco Webex Calling Dedicated Instance, la cual podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de los dispositivos afectados.

Esta vulnerabilidad se origina debido a una validación incorrecta de la información proporcionada por el usuario en las solicitudes HTTP. Un atacante podría explotarla

mediante el envío de una secuencia de solicitudes HTTP especialmente manipuladas a la interfaz de administración web del dispositivo. Una explotación exitosa permitiría al atacante obtener acceso como usuario al sistema operativo subyacente y, posteriormente, elevar privilegios hasta nivel root.

Cisco ha asignado a este aviso de seguridad una Calificación de Impacto de Seguridad (SIR) Crítica, en lugar de Alta, debido a que la explotación de esta vulnerabilidad puede resultar en la elevación de privilegios a root, lo que representa un riesgo significativo para la integridad y seguridad de los sistemas afectados.

Cisco ha publicado actualizaciones de software que corrigen esta vulnerabilidad. No existen soluciones alternativas para mitigar el riesgo, por lo que se recomienda aplicar las actualizaciones correspondientes a la mayor brevedad posible.

El descubrimiento de la vulnerabilidad CVE-2026-20045 se produce menos de una semana después de que Cisco publicara actualizaciones para otra vulnerabilidad crítica explotada activamente, que afecta a AsyncOS Software para Cisco Secure Email Gateway y Cisco Secure Email and Web Manager (CVE-2025-20393, puntuación CVSS: 10.0), la cual también podría permitir la ejecución de comandos arbitrarios con privilegios de root.

## IV. VECTOR DE ATAQUE.

**CVE-2026-20045**: es una vulnerabilidad crítica de ejecución remota de código causada por una validación incorrecta de la entrada proporcionada por el usuario en solicitudes HTTP enviadas a las interfaces de administración de Cisco Unified Communications.

## V. IMPACTO

- **Cisco Unified Communications Manager (CSCwr21851)**: utilizado principalmente por grandes empresas, agencias gubernamentales y del sector público, y organizaciones en industrias reguladas que ejecutan su propia infraestructura de telefonía empresarial.
- **Cisco Unified Communications Manager Session Management Edition (CSCwr21851)**: utilizado principalmente por grandes empresas con múltiples clústeres CUCM, implementaciones regionales o complejidad de enrutamiento global.

- **Cisco Unified Communications Manager IM & Presence Service (CSCwr29216)**: utilizado por organizaciones que desean presencia y mensajería en tiempo real integradas con la telefonía.
- **Cisco Unity Connection (CSCwr29208)**: para organizaciones que necesitan correo de voz y mensajería empresarial vinculados a su infraestructura de llamadas.
- **Instancia dedicada de Cisco Webex Calling (CSCwr21851)**: para organizaciones que desean una versión privada y alojada en la nube de llamadas estilo CUCM.

## VI. RECOMENDACIONES:

- Identificar si existen sistemas afectados en el entorno.
- Aplicar de forma inmediata las actualizaciones recomendadas por Cisco.
- Restringir el acceso a las interfaces de administración web mientras se ejecuta el proceso de actualización.
- Revisar registros del sistema y de acceso HTTP en busca de actividad sospechosa.

## VII. 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.

## VIII. REFERENCIAS.


- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b
- https://securityaffairs.com/187177/security/cisco-fixed-actively-exploited-unified-communications-zero-day.html
- https://www.helpnetsecurity.com/2026/01/21/cisco-enterprise-communications-cve-2026-20045/
- https://socradar.io/blog/cve-2026-20045-cisco-unified-communications-0-day/
- https://nvd.nist.gov/vuln/detail/CVE-2026-20045
- https://thehackernews.com/2026/01/cisco-fixes-actively-exploited-zero-day.html