BOLETÍN DE ALERTA

Boletín Nro.: 2024-06
Fecha de publicación: 25/01/2024
Tema: Vulnerabilidad de ejecución remota de código *RCE* en productos Cisco Unified Communications y Contact Center Solutions

Productos afectados:

- Packaged Contact Center Enterprise (PCCE)(CSCwe18830)
  - Versiones afectadas 12.0 y anteriores, 12.5(1) y 12.5(2)
- Unified Communications Manager (Unified CM)(CSCwd64245)
  - Versiones afectadas 11.5(1),12.5(1) y 14
- Unified Communications Manager IM & Presence Service (Unified CM IM&P) (CSCwd64276)
  - Versiones afectadas 11.5(1),12.5(1) y 14
- Unified Communications Manager Session Management Edition (Unified CM SME) (CSCwd64245)
  - Versiones afectadas 11.5(1),12.5(1) y 14
- Unified Contact Center Express (UCCX)(CSCwe18773)
  - Versiones afectadas 12.0 y anteriores y 12.5(1)
- Unity Connection (CSCwd64292)
  - Versiones afectadas 11.5(1), 12.5(1) y 14
- Virtualized Voice Browser (VVB) (CSCwe18840)
  - Versiones afectadas 12.0 y anteriores, 12.5(1) y 12.5(2)

Descripción:

Cisco ha reportado una vulnerabilidad identificada como CVE-2024-20253 con puntuación CVSS de 9.9 (Severidad Crítica) que permite a un atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web. Esta vulnerabilidad, se debe al procesamiento inadecuado de los datos proporcionados por el usuario que se leen en la memoria.

Impacto:

Esta vulnerabilidad podría permitir a un actor malicioso ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web. Con acceso al sistema operativo subyacente, el atacante también podría establecer acceso root en el dispositivo afectado.
Cisco ha informado que, hasta el momento, no hay evidencia de que la vulnerabilidad está siendo explotada activamente.

Recomendación:

Se recomienda instalar las actualizaciones que Cisco ha lanzado para corregir estas vulnerabilidades disponibles en su sitio web oficial.

En caso de no poder realizar la actualización, como medida alternativa se puede mitigar estableciendo Listas de Control de Acceso (ACL) en dispositivos intermedios que separan del cluster de Comunicaciones Unificadas o Soluciones de Contact Center de los usuarios y el resto de la red, para permitir el acceso solo a puertos de los servicios implementados.

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ejecucion-remota-de-codigo-en-productos-de-cisco
- https://securityonline.info/cve-2024-20253-cvss-9-9-cisco-unified-communications-products-rce-vulnerability/