Cisco Systems implementó actualizaciones de seguridad para una vulnerabilidad crítica que afecta al Portal de Administración del Centro de Contacto Unificado (CCMP) y el Administrador de Dominio del Centro de Contacto Unificado (CCDM), que podría ser explotada por un atacante remoto para tomar el control de un sistema afectado.

Rastreada como CVE-2022-20658, la vulnerabilidad fue clasificada con una gravedad de 9.6 en el sistema de puntuación CVSS, y se refiere a una falla en la escalada de privilegios que surge de la falta de validación del lado del servidor de los permisos de usuario que podría utilizarse como arma para crear cuentas de administrador no autorizadas enviando una solicitud HTTP especialmente diseñada.

> *«Con estas cuentas, el atacante podría acceder y modificar la telefonía y los recursos de los usuarios en todas las plataformas unificadas que están asociadas al vulnerable Cisco Unified CCMP. Para explotar con éxito esta vulnerabilidad, un atacante necesitaría credenciales de usuario avanzado válidas»*, dijo Cisco en un aviso publicado esta semana.

Las versiones de producto Unified CCMP y Unified 12.5.1, 12.0.1 y 11.6.1 y anteriores que se ejecutaron con la configuración predeterminada se ven afectadas, dijo la compañía de equipos de red, y agregó que encontró el problema como parte del soporte del Centro de Asistencia Técnica (TAC). La versión 12.6.1 del software no se ve afectada.

Aunque no hay evidencia de que la vulnerabilidad haya sido explotada en ataques en el mundo real, se recomienda que los usuarios actualicen a la última versión para mitigar el riesgo asociado con las fallas.