CSIRTSALUD-AL-20250808-11

TLP: CLEAR

Incidente Id	0011
Fecha del reporte	08/08/2025
Entidad	Todas las entidades del ecosistema digital
Título	Nueva vulnerabilidad en Microsoft Exchange Server permite escalada de privilegios a administradores
Herramienta de detección	Análisis de fuentes oficiales (Microsoft)
Activo involucrado	Servidores Microsoft Exchange en configuraciones híbridas (2016, 2019, Subscription Edition)
Tipo de incidente	Vulnerabilidad Crítica
Nivel de riesgo	Alto

Descripción:

El equipo CSIRT Salud alerta sobre una vulnerabilidad crítica (CVE-2025-53786) en Microsoft Exchange Server, documentada oficialmente el 6 de agosto de 2025. Esta falla permite a atacantes con acceso administrativo local escalar privilegios en entornos cloud sin dejar rastros detectables fácilmente, comprometiendo la integridad de Exchange Online.

La vulnerabilidad explota tokens de acceso especiales en despliegues híbridos, los cuales no pueden revocarse durante 24 horas una vez robados. Investigadores demostraron en Black Hat 2025 cómo modificar contraseñas de usuarios, convertir cuentas cloud a híbridas e impersonar identidades.

Riesgos asociados

La explotación de esta vulnerabilidad conlleva riesgos críticos para la seguridad organizacional, especialmente en entornos híbridos. Estos incluyen la escalada de privilegios hacia la nube, la persistencia silenciosa de atacantes y el compromiso de identidades privilegiadas, lo que podría derivar en brechas de datos o incumplimientos normativos. A continuación, se explican técnicamente estos riesgos y su impacto potencial.

Riesgo	Descripción
Escalada de privilegios en la nube	Atacantes con acceso administrativo local pueden extender privilegios a Microsoft 365, evadiendo auditorías.
Persistencia en entornos híbridos	Tokens no revocables permiten acceso prolongado (24h) para robo de datos o movimientos laterales.
Compromiso de identidades	Modificación de permisos ejecutivos o creación de backdoors entre sistemas on-premise y cloud.
Incumplimiento normativo	Violación de estándares como ISO 27001 o GDPR debido a brechas en la gestión de identidades.

Vector de ataque:

Explotación directa: Uso de tokens válidos para impersonar usuarios híbridos.

Movimiento lateral: Acceso a recursos cloud críticos desde servidores Exchange comprometidos.

Ataques de fuerza bruta: Combinado con credenciales administrativas robadas.

Productos afectados:

A continuación, se detallan las versiones específicas de Microsoft Exchange Server vulnerables a **CVE-2025-53786**, junto con sus respectivos builds afectados. Es fundamental verificar si los servidores en su entorno coinciden con estas versiones para priorizar la aplicación de parches y configuraciones de mitigación.

Producto	Builds Afectados
Exchange Server 2019 CU15	15.02.1748.024
Exchange Server 2019 CU14	15.02.1544.025
Exchange Server 2016 CU23	15.01.2507.055
Exchange Server Subscription Edition	15.02.2562.017

Recomendaciones de mitigación:

1. **Aplicar actualizaciones**:
   - Instalar el *Hotfix* de abril 2025 en servidores Exchange afectados (ver builds en tabla adjunta).
   - Seguir la guía de Microsoft para implementar aplicaciones híbridas dedicadas.
2. **Configuraciones críticas**:
   - Ejecutar el *Exchange Health Checker* para validar el estado de los service principals.
   - Habilitar el *Modo de Limpieza de Service Principals* para resetear keyCredentials.
3. **Controles compensatorios**:
   - Restringir privilegios administrativos en servidores Exchange.
   - Monitorizar logs de autenticación híbrida con herramientas SIEM/EDR.
4. **Inventario y priorización**:
   - Identificar servidores Exchange en despliegues híbridos (versiones afectadas: 2016 CU23, 2019 CU14/CU15, Subscription RTM).

Fuentes:

- https://cybersecuritynews.com/microsoft-exchange-server-vulnerability/
- https://www.tenable.com/blog/cve-2025-53786-frequently-asked-questions-about-microsoft-exchange-server-hybrid-deployment