Boletín de alerta

Boletín Nro.: 91
Fecha de publicación: 26/08/2026
Tema: Alerta 2026-91 Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Microsoft Exchange Server 2016 CU23 (x64): versiones desde 15.01.0.0 hasta antes de **15.01.2507.072**.
- Microsoft Exchange Server 2019 CU14 (x64): versiones desde 15.02.0.0 hasta antes de **15.02.1544.044**.
- Microsoft Exchange Server 2019 CU15 (x64): versiones desde 15.02.0.0 hasta antes de **15.02.1748.049**.
- Microsoft Exchange Server Subscription Edition (SE) RTM (x64): versiones desde 15.02.0.0 hasta antes de **15.02.2562.046**.

Descripción

Recientemente, Microsoft reveló la vulnerabilidad CVE-2026-62911, reportada por Orange Tsai, del equipo DEVCORE Research Team, en Microsoft Exchange Server, plataforma local de correo electrónico, calendario y colaboración empresarial. La vulnerabilidad posee una severidad alta, con puntuación CVSS v3.1 de 8.0 y puede permitir que un atacante autenticado con pocos privilegios eleve sus permisos a través de la red.

La vulnerabilidad se clasifica como CWE-294: bypass de autenticación mediante captura y repetición (capture-replay). Un atacante puede reutilizar una solicitud o material de autenticación previamente capturado para eludir los controles de autenticación previstos, lo que habilita el acceso con privilegios superiores dentro de Exchange.

El análisis publicado por Zero Day Initiative indica que el problema reside en el procesamiento de solicitudes de autorización y en una gestión inadecuada de sesiones. En un escenario de explotación, esta condición puede encadenarse con otras vulnerabilidades para alcanzar ejecución de código bajo el contexto de SYSTEM, comprometiendo confidencialidad, integridad y disponibilidad del servidor.

No hay evidencia pública de explotación activa al momento de la publicación. Sin embargo, CISA clasifica el impacto técnico potencial como total; por ello, los servidores Exchange expuestos o de alta criticidad deben priorizarse en el ciclo de parcheo.

Solución:

Microsoft corrigió la vulnerabilidad mediante las actualizaciones de seguridad publicadas de **agosto de 2026**. Se recomienda aplicar de inmediato el Security Update correspondiente y comprobar que el servidor alcance, como mínimo, las compilaciones corregidas indicadas anteriormente.

Para Exchange Server 2019 CU15, instalar KB5121574. Para Exchange Server 2016 CU23, instalar KB5121576. Las actualizaciones para Exchange SE y Exchange 2019 CU14 están disponibles en el boletín de actualizaciones de seguridad de agosto de 2026.

Exchange Server 2016 y 2019 ya se encuentran fuera de soporte general; las actualizaciones de agosto de 2026 requieren pertenecer al programa Extended Security Updates (ESU), período 2. Las organizaciones que no cuenten con ESU deben planificar la migración a Exchange Server Subscription Edition. Tras actualizar, se recomienda ejecutar el Exchange Server Health Checker para validar la instalación y revisar configuraciones adicionales.

Como medidas de reducción de exposición, limite el acceso a Exchange únicamente a redes y usuarios necesarios, aplique mínimo privilegio a las cuentas, supervise eventos de autenticación y autorización anómalos y analice solicitudes repetidas o sesiones inusuales.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911
- https://www.zerodayinitiative.com/advisories/ZDI-26-538/
- https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates