

Alert Bulletin

Bulletin N.: 56

Publication Date: 11/07/2025

Subject: Alerta 2025-56 Vulnerabilidades importantes en SPNEGO y SQL Server de Microsoft.

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Agente de Azure Monitor
- Sistema de archivos de intermediación de Microsoft
- Microsoft Edge (basado en Chromium)
- Suite Microsoft Office y Teams
- Administrador de PC de Microsoft
- Servidor SQL
- Pymes de Windows
- Negociación extendida de Windows SPNEGO

y en otros productos

Descripción

Se ha reportado una vulnerabilidad crítica denominada CVE-2025-47981 con un score 9.8, de tipo RCE que afecta al componente SPNEGO Extended Negotiation (NEGOEX) Security Mechanism. Además, se han publicado en total 130 vulnerabilidades que afectan a varios productos de Microsoft en su último Microsoft's Patch Tuesday.

Dicha vulnerabilidad CVE-2025-47981, es un desbordamiento de búfer basado en montón (Head Buffer Overflow) en SPNEGO Extended Negotiation de Windows permite que un atacante no autorizado ejecute código a través de una red.

De todas las vulnerabilidades publicadas, 53 de estas deficiencias se clasifican como errores de escalada de privilegios, seguidos de 42 como ejecución remota de código, 17 como divulgación de información y 8 como omisiones de funciones de seguridad.

Estos parches se suman a otras dos vulnerabilidades corregidas por la compañía en el navegador Edge.

Otra vulnerabilidad corregida importante que se menciona como públicamente conocida es una falla de divulgación de información en Microsoft SQL Server (CVE-2025-49719 , puntuación CVSS: 7,5) que podría

permitir que un atacante no autorizado pierda memoria no inicializada.

Para ver el listado de todas las vulnerabilidades publicadas puede dirigirse al siguiente enlace:

<https://msrc.microsoft.com/update-guide/releaseNote/2025-Jul>

Solución:

Se recomienda aplicar los parches de seguridad publicados por el fabricante.

Información adicional:

- <https://nvd.nist.gov/vuln/detail/CVE-2025-47981>
- <https://msrc.microsoft.com/update-guide/releaseNote/2025-Jul>