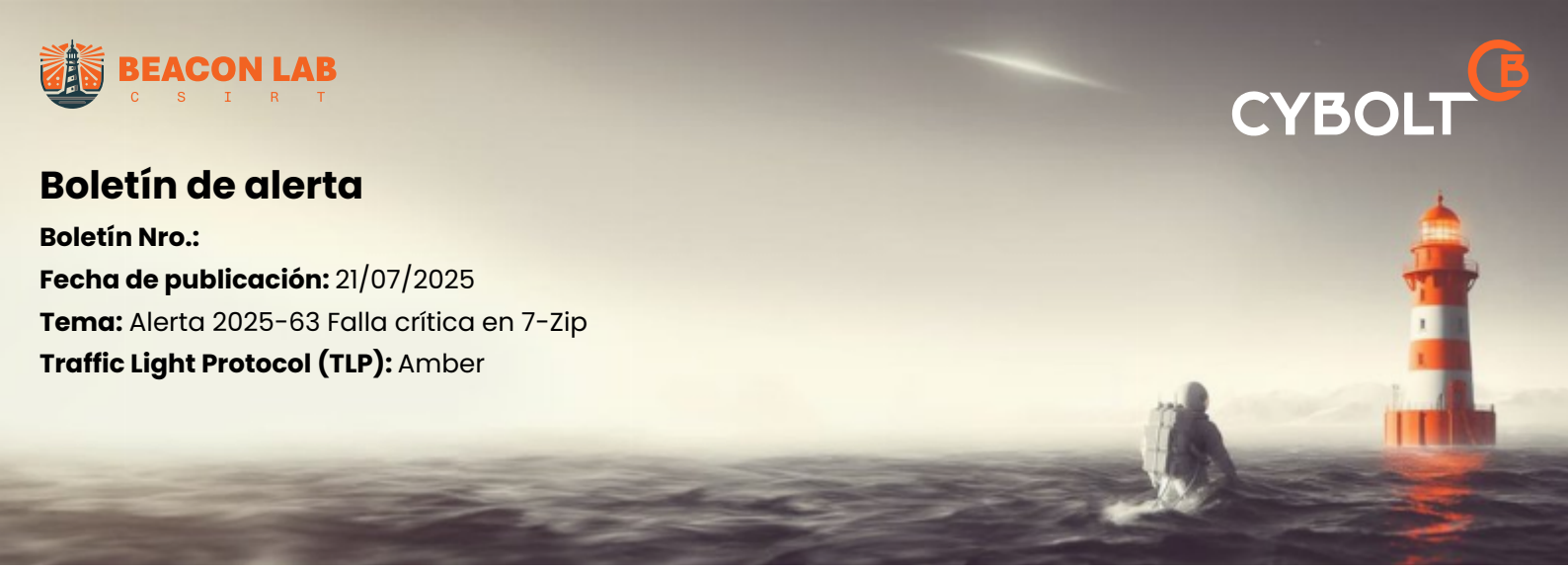

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 21/07/2025
Tema: Alerta 2025-63 Falla crítica en 7-Zip
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- 7-Zip (versiones anteriores a la 25.0.0)

Descripción

Se han identificado dos vulnerabilidades de seguridad en 7-Zip, una de las herramientas de compresión de archivos más populares del mundo. Estas fallas afectan a las versiones anteriores a la 25.0.0 y, aunque no permiten ejecutar código malicioso de forma remota, sí podrían provocar problemas graves como daños en la memoria del sistema o bloqueos inesperados de la aplicación.

La primera vulnerabilidad (CVE-2025-53816) se relaciona con el mal manejo de archivos en formato RAR5. En situaciones específicas, al descomprimir estos archivos, 7-Zip puede escribir datos fuera de los límites seguros de la memoria. Esto puede ocasionar fallos en la aplicación o congelamientos, generando riesgo de denegación de servicio.

La segunda vulnerabilidad (CVE-2025-53817) afecta la forma en que 7-Zip procesa ciertos archivos de documentos compuestos. Si se manipulan de manera maliciosa, podrían hacer que la aplicación se cierre de forma inesperada, afectando los procesos de trabajo que dependan de ella.

Solución:

En caso de que 7zip esté presente en su infraestructura como componente de otro software, consulte la disponibilidad de parches al fabricante de dicho software

Actualiza 7-Zip a su **versión más reciente (25.0.0)**, la cual **corrige ambas vulnerabilidades**

https://www.7-zip.org

Información adicional:

- Dos vulnerabilidades en 7-Zip podrían desencadenar una denegación de servicio

- GHSL-2025-058: Denegación de servicio (DoS) debido a daños en la memoria en 7-Zip – CVE-2025-53816 | Laboratorio de seguridad de GitHub
- oss-security – CVE-2025-53816: Memory corruption in 7-Zip before 25.00