Samsung ha lanzado actualizaciones de software para corregir una vulnerabilidad crítica en MagicINFO 9 Server, la cual ha sido explotada activamente.

El fallo de seguridad, identificado como CVE-2025-4632 (con una puntuación CVSS de 9.8), es un problema de traversal de directorios, lo que permite a los atacantes escribir archivos arbitrarios con permisos de sistema.

> Según el informe oficial, *«La limitación incorrecta de una ruta de acceso a un directorio restringido en Samsung MagicINFO 9 Server, en versiones anteriores a la 21.1052, permite que los atacantes escriban archivos como autoridad del sistema.»*

Cabe destacar que CVE-2025-4632 es una variante del fallo CVE-2024-7399, corregido por Samsung en agosto de 2024. Sin embargo, tras la publicación de un proof-of-concept (PoC) por SSD Disclosure el 30 de abril de 2025, esta nueva vulnerabilidad ha sido explotada en algunos casos para desplegar el botnet Mirai.

Inicialmente se pensó que los ataques apuntaban a CVE-2024-7399, pero la empresa de ciberseguridad Huntress descubrió que el fallo seguía presente incluso en servidores MagicINFO 9 con la versión más reciente (21.1050).

En un informe publicado el 9 de mayo, Huntress reveló que se identificaron tres incidentes en los que actores desconocidos ejecutaron los mismos comandos para descargar archivos como «srvany.exe» y «services.exe» en dos sistemas, y realizar tareas de reconocimiento en un tercero.

Los usuarios de MagicINFO 9 Server deben aplicar las correcciones más recientes lo antes posible para evitar riesgos de seguridad.

> *«Hemos verificado que MagicINFO 9 21.1052.0 mitiga el problema original identificado en CVE-2025-4632″,* comentó Jamie Levy, director de tácticas de

> adversarios en Huntress, en una declaración.
>
> *«Cualquier máquina con las versiones v8 – v9 21.1050.0 seguirá afectada por esta vulnerabilidad. También descubrimos que actualizar de MagicINFO v8 a v9 21.1052.0 no es tan simple, ya que primero se debe actualizar a 21.1050.0 antes de aplicar el parche final.»*