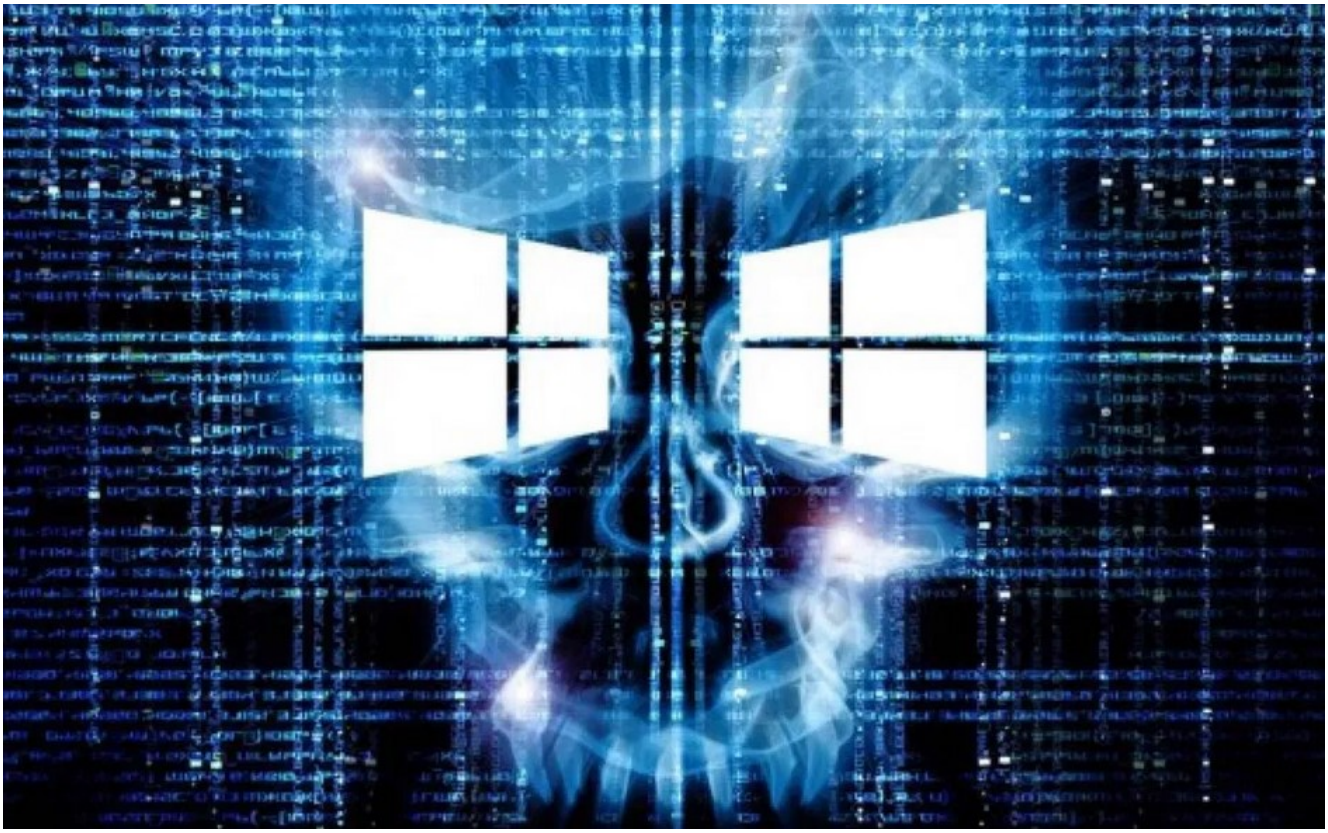
Windows tiene dos fallos de seguridad importantes, están siendo explotados actualmente

Un error en el formato binario de los accesos directos de Windows y otro error en Windows Server son dos grandes dolores de cabeza de Microsoft que aún no son solucionados, para su desgracia son fallos explotados a gran escala

Windows tiene un problema enorme de seguridad, concretamente en dos vulnerabilidades que no han sido corregidas del todo. Una de ellas es de tipo “día cero” que está siendo explotada desde el 2017, además de un fallo crítico que intentó ser solucionado sin éxito. Los ataques han ido en aumento en una gran parte de internet. Lo que reporta Ars Technica es que se trata de una operación coordinada a gran escala que parece no tener final. En Windows 11 fue encontrado uno que data desde 2023 y tardaron un año en resolverlo y otro que permitía la instalación del sistema en ordenadores no compatibles.



Dos fallos increíbles que vulneran la seguridad en Windows, uno desde el 2017, no han sido solucionados

La vulnerabilidad del “día cero” no fue descubierto hasta el pasado mes de marzo. La empresa de seguridad Trend Micro descubrió que había sido explotada desde 2017 por diferentes grupos de amenazas. Algunos están vinculados a estados nación del mundo. La vulnerabilidad reconocida como “ZDI-CAN-25373” instalan cargas útiles en infraestructuras de más de 60 países. Estamos a finales de año y Microsoft no ha podido contra este fallo. Su origen radica en el formato binario de los accesos directos de Windows. Lo que provoca es que agiliza la apertura de apps o el acceso a archivos invocados por dicho archivo binario sin necesidad de encontrar su ubicación.

Una de sus variantes, vinculada a un grupo chino, explota la vulnerabilidad contra países europeos; un troyano de acceso remoto llamado “PlugX”. La vulnerabilidad se disfraza de un

formato RC4 para poder avanzar hasta su meta y desenvolverse. Aunque no exista un parche definido para este tipo de vulnerabilidad, los usuarios pueden protegerse restringiendo las funciones de los archivos .ink cuando se bloquean o se limita su uso en orígenes que no sean confiables. Esto es posible configurando el Explorador de Windows.

El segundo fallo tiene que ver con la ejecución remota de código en los servicios de actualización de Windows Server. Se estaba propagando mediante un “gusano informático” causado en un fallo de serialización. Aparentemente ya fue solucionada con una actualización no programada pero después se demostró que la solución no estaba completada. Se volvió a explotar, una empresa de seguridad indicó que la vulnerabilidad había sido detectada. El nombre del fallo ha sido bautizado como “CVE-2025-59287”. Los objetivos son servidores WSUS que están presentes en internet. El fallo más relevante rebautizado como “CVE-2025-9491” (del día cero) aún no tiene una fecha aparente para solucionarse.

Fuente: andro4all.