Microsoft publicó el martes una mitigación para una vulnerabilidad de evasión de BitLocker denominada *YellowKey*, tras su divulgación pública la semana pasada.

La falla de día cero, ahora identificada como CVE-2026-45585, posee una puntuación CVSS de 6.8 y ha sido clasificada como un mecanismo para eludir funciones de seguridad de BitLocker.

«Microsoft tiene conocimiento de una vulnerabilidad de omisión de funciones de seguridad en Windows conocida públicamente como 'YellowKey'», señaló la compañía en un aviso oficial. *«La prueba de concepto de esta vulnerabilidad fue divulgada públicamente, incumpliendo las mejores prácticas de divulgación coordinada de vulnerabilidades.»*

El problema afecta a Windows 11 versión 26H1 para sistemas basados en x64, Windows 11 versión 24H2 para sistemas x64, Windows 11 versión 25H2 para sistemas x64, Windows Server 2025 y Windows Server 2025 (instalación Server Core).

YellowKey fue revelada por un investigador de seguridad llamado Chaotic Eclipse. El método consiste en colocar archivos especialmente diseñados denominados "FsTx" en una unidad USB o en una partición EFI, conectar el dispositivo al equipo Windows objetivo con BitLocker habilitado, reiniciar en el entorno de recuperación de Windows (WinRE) y ejecutar una consola con acceso sin restricciones manteniendo presionada la tecla CTRL.

«Si realizaste correctamente todos los pasos, se abrirá una consola con acceso irrestricto al volumen protegido por BitLocker», explicó el investigador en una publicación de GitHub.

Microsoft indicó que una explotación exitosa permitiría a un atacante con acceso físico evitar la protección de cifrado BitLocker del dispositivo de almacenamiento del sistema y acceder a la información cifrada.

«Para comprometer el cifrado, YellowKey aprovecha una suposición de confianza en la interfaz de recuperación, permitiendo a los atacantes iniciar una consola sin restricciones y con acceso total al volumen cifrado durante la secuencia de recuperación previa al

arranque», señaló LevelBlue. *«Y debido a que YellowKey no requiere instalación de software, credenciales existentes ni acceso a la red para vulnerar el cifrado, cualquier equipo con un puerto USB y capacidad de reinicio puede convertirse en un objetivo.»*

Para reducir el riesgo, se recomendaron las siguientes medidas de mitigación:

- Montar la imagen WinRE en cada dispositivo.
- Montar el hive del registro del sistema de la imagen WinRE montada.
- Modificar BootExecute eliminando el valor *«autofstx.exe»* de la entrada REG_MULTI_SZ BootExecute del Session Manager.
- Guardar y descargar el hive del registro.
- Desmontar y confirmar la imagen WinRE actualizada.
- Restablecer la confianza de BitLocker para WinRE.

«En concreto, se evita que la utilidad de recuperación automática FsTx, autofstx.exe, se ejecute automáticamente cuando se inicia la imagen WinRE», explicó el investigador de seguridad Will Dormann. *«Con este cambio, la reproducción transaccional de NTFS que elimina winpeshl.ini deja de producirse. También se recomienda migrar de TPM-only a TPM+PIN.»*

Microsoft también destacó que los usuarios pueden protegerse contra este tipo de explotación configurando BitLocker en dispositivos ya cifrados que utilizan el modo *"TPM-only"* y cambiándolo a *"TPM+PIN"* mediante PowerShell, línea de comandos o el panel de control. Esto obliga a introducir un PIN durante el arranque para descifrar la unidad, bloqueando de forma efectiva los ataques YellowKey.

En los dispositivos que aún no cuentan con cifrado, se aconseja a los administradores habilitar la opción *"Require additional authentication at startup"* mediante Microsoft Intune o Políticas de Grupo, y verificar que la configuración *"Configure TPM startup PIN"* esté establecida en *"Require startup PIN with TPM"*.