Windows' 'rescue' feature becomes a door for hackers to steal data

Attackers can exploit these vulnerabilities to bypass BitLocker and steal protected data.

At Black Hat USA 2025 and DEF CON 33, Microsoft's Security Testing & Offensive Research (STORM) team disclosed a series of new vulnerabilities in the Windows Recovery Environment (WinRE). Attackers can exploit these vulnerabilities to bypass BitLocker and steal protected data.

What's worrying is that WinRE is one of the core features of Windows, easily accessible by holding down the Shift key and selecting Restart right from the Windows login screen.

What is BitLocker?

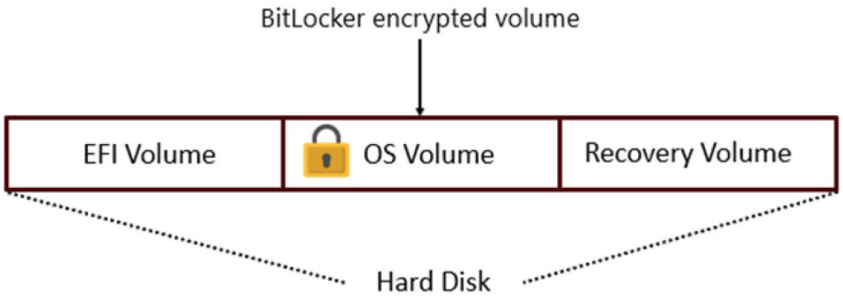
BitLocker (also known as Device Encryption – DE) is a full-disk encryption feature of Windows, which helps protect data from the risk of unauthorized access, especially in case the device falls into the wrong hands.

After BitLocker was released, Microsoft changed WinRE so that it could still recover the system even if the operating system drive was encrypted. The changes included:

1. Move the WinRE.wim file from the encrypted operating system partition to the unencrypted recovery partition so that it can be accessed in case of a crash.
2. Implement Trusted WIM Boot to verify the WinRE file before automatically unlocking the OS drive.
3. Add a mechanism to re-lock the drive if the user opens 'dangerous' tools like Command Prompt, requiring re-entering the BitLocker recovery key to access.

However, the STORM team said that after Trusted WIM Boot passes the authentication step, WinRE will be in an auto-unlock state, allowing data to be read from unprotected partitions, such as the EFI partition or the recovery partition. This process inadvertently opens up many new vulnerabilities.

To prevent this, Microsoft recommends that users: Enable TPM with PIN for pre-boot authentication, reducing dependence on auto-unlock mechanism. At the same time, activate REVISE (KB5025885) to prevent downgrade attacks.



These vulnerabilities are currently tracked as CVE-2025-48800, CVE-2025-48003, CVE-2025-48804, and CVE-2025-48818, and have been patched on Windows 11 and Windows 10 with the July 2025 Patch Tuesday. Since patches are cumulative, you can also download and install the latest August Patch for Windows 11 (KB5063878, KB5063875) and Windows 10 (KB5063709/KB5063877/KB5063871/KB5063889) that were recently released.