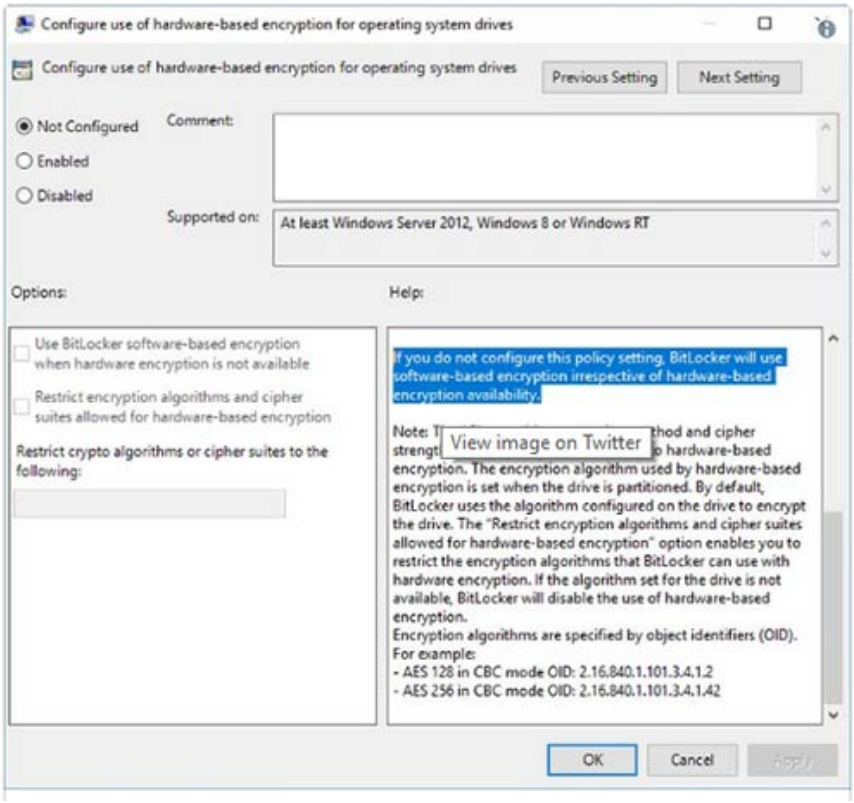
Microsoft changes the default settings to keep the content stored on the hard drive safe

In June last year, security researchers discovered that the method of securing SSD hard drive encryption could be easily 'broken' ...

In June last year, security researchers discovered that the method of securing SSD hard drives could be easily "broken" by just $ 100 worth of tools, along with The simple way is to restart the drive's firmware.Specifically, this vulnerability allows hackers to access the drive and transfer data without using a password.Soon after, Microsoft shared a step-by-step process for the system administrator to switch from hardware-based encryption to software-based encryption, but that's just a 'fire-fighting' measure.This vulnerability affects most major SSD manufacturers and includes Crucial MX100, MX200 and MX3000 drives, Samsung T3 and T5, and Samsung 840 Evo and 850 Evo.



1. The first Windows 10 build for foldable computers appeared on Microsoft servers

The problem only affects hardware encryption, not software encryption, and Bitlocker has been found to be a particularly vulnerable part when using hardware encryption (also called self-encryption), Based on self-coding and accurate decoding of SSD.

Since the time Microsoft asked users to switch to software encryption to protect their data, until now, in the latest version of Windows 10 19H1, Microsoft seems to have switched to code to use software by default.

According to Tero Alhonen's tweet, if your SSD previously supported hardware encryption, Windows 10 will boot by default in that mode because it is faster and less resource-intensive, but now, GPOs The new default will be software encryption.

1. Microsoft launched a video reminding Windows 7 "death" and advised users to upgrade to Windows 10

If you really care about the security of data to use BitLocker, you may want to check if you're using software or hardware encryption.To do that, follow these steps:

Step 1: Start the command prompt with administrator privileges by opening the **Start** menu, entering the **cmd.exe** search keyword, then right-clicking on the result and selecting the **Run as administrator option.**

Step 2: Confirm the UAC prompt when it is displayed.

Step 3: Enter the command **manage-bde.exe -status.**

Step 4: Check whether the **Encryption Method** displays **Hardware Encryption** content in the **Encryption Method** section.

If there is no Hardware Encryption reference information in the returned results, it means that your system is using Software Encryption.

If the system is using hardware encryption you want to switch to software encryption, you will need to decrypt the drive and re-encrypt it from scratch.

The problem will only affect SSDs, not HDDs, but then they almost become the default in mid-range and higher laptops.

See more:

1. From now on, Windows 10 will automatically allocate at least 7GB of space on the system for updating the new version
2. There were Windows 10 build 18312 with many improvements for the operating system, invited to download ISO files and experience
3. Microsoft wants to 'death' technology using passwords on Windows 10
4. Beyond Windows 7, Windows 10 becomes the most commonly used operating system in the world