38C3: Bitlocker bypassed via vulnerabilities (Dec. 2024)

Posted on 2024-12-31 by guenni

[German]A small addendum from the weekend – at the 38C3 congress of the Chaos Computer Club, Thomas Lambertz, a security expert, showed how Microsoft's Bitlocker encryption can be circumvented by "downgrading" a patched vulnerability. The way in which secret services or law enforcement agencies can gain access to encrypted data.

Microsoft propagates the encryption of data entries on Windows systems using Bitlocker. This is intended to protect confidential data from unauthorized third parties. However, Bitlocker can present a number of hurdles for users (see links at the end of the article, as well as the following screenshot from the 38C3 session).

Problems with Bitlocker, screenshot at 45:13 from the presentation at 38C3, including reference to my article Windows 10/11 updates (e.g. KB5040442) trigger Bitlocker queries (July 2024)

It is also noticeable that Bitlocker repeatedly shines through vulnerabilities that make it possible to circumvent the encryption. For example, I reported on such an approach, albeit a more elaborate one, in the article Windows Bitlocker-Verschlüsselung trotz TPM ausgehebelt and Bitlocker key determined via TPM within 42 seconds with Raspberry Pi Pico.

However, forensics companies such as Cellebrite, which support law enforcement agencies, or secret services and the judiciary have probably found ways of decrypting encrypted data carriers using various approaches. So it was only a matter of time before security researchers took a closer look at Bitlocker.

Bitlocker bypassed by software

Security expert Thomas Lambertz held a session at the 38 Chaos Computer Congress (38C3) entitled Windows BitLocker: Screwed without a Screwdriver, in which he showed how he was able to use a Windows vulnerability and a modified Linux to access an encrypted Bitlocker drive under a current and fully patched Windows 11 without knowing the recovery key.

The background to this is the Microsoft Bitlocker implementation for the complete encryption of a volume (data carrier, partition), which offers several operating modes. Secure Boot-based encryption is most commonly used by private and corporate customers. In newer Windows 11 installations, the so-called device encryption is activated by default (see also Windows 10/11 Home Edition and the OEM Bitlocker pitfall).

In this mode, the hard disk is encrypted by Bitlocker in hibernation mode, but is automatically unsealed when a legitimate Windows is booted. The user does not need a separate decryption password as this is taken from the TPM during Secure Boot. Users simply have to log in to their normal Windows user account.

The exciting question now is: Is it possible to access the data on Bitlocker-encrypted devices without knowing the password? The presentation at 38C3 demonstrated how BitLocker encryption can be bypassed on a current Windows 11 system with Secure Boot.

This is possible despite protection by Secure Boot because a little-known software vulnerability – bitpixie (CVE-2023-21563) – can be exploited. This vulnerability was patched by Microsoft in November 2022 (it has been known since 2023). But CVE-2023-21563 can still be exploited today with a downgrade attack to decrypt BitLocker.

Specifically, an outdated Windows boot loader is loaded under Secure Boot in order to start Windows in safe mode. This causes the Bitlocker recovery key (known as the volume mount key, VMK) to be loaded into the computer's RAM.

A Linux system is then started on a second computer, which is connected to

the first Windows computer via LAN, using Secure Boot. A memory dump of the Windows working memory is created via the network. The key required to mount the Bitlocker drive can then be extracted from this dump. You then have access to the data on the Bitlocker drive without ever having received the user's logon password or the recovery key.

The details can be found in the recording of the 38C3 session available under Windows BitLocker: Screwed without a Screwdriver (some information from the video can be found here).

Similar articles:

Windows Bitlocker recovery key query bug fixed by August 2024 updates
Microsoft confirms Bitlocker queries through Windows July 2024 updates
Windows 10/11 updates (e.g. KB5040442) triggers Bitlocker queries (July 2024)
Windows WinRE update (for Bitlocker Bypassing vulnerability CVE-2024-20666) fails with installation error 0x80070643 (Jan. 2024, KB5034441)
Windows 10/11: Microsoft has published a fix for OOBE Bitlocker Bug
Windows 10/11: Microsoft releases script for WinRE BitLocker bypass fix
Windows 10/11 Home Edition and the OEM Bitlocker pitfall
Bitlocker key determined via TPM within 42 seconds with Raspberry Pi Pico
Windows 10/11: Bitlocker Error 65000 in MDM fixed
Question: Where does Bitlocker store the recovery key in Windows?