EVIDEN
an atos business

Security Bulletin

BitLocker vulnerability

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1084**
Created	:	**12 February 2024**
Version	:	**0.1**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**5 March 2024**
Keywords	:	**Bitlocker, TPM**

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

DRAFT - DO NOT SHARE EXTERNALLY

List of changes

Version	Date	Description
0.1	2024/03/05	Initial neutralization bulletin

Executive summary

The encryption of BitLocker was compromised by Stacksmashing, a Youtuber who released a video explaining the method he used to intercept BitLocker data, extract decryption keys, and effectively exploit the BitLocker encryption process.

Youtuber exploit revolves around the external Trusted Platform Module (TPM), which is the very same TPM chip responsible for preventing Windows 11 upgrades on certain laptops and computers. Numerous motherboards incorporate the TPM chip and contemporary CPUs seamlessly integrate it into their design, there are still other machines that rely on an external TPM.

External TPMs can establish communication with the CPU through an LPC bus (Low Pin Count), which serves as a means for low-bandwidth devices to interact with other hardware without causing any performance burden.

The Youtuber discovered that although the data stored on the TPM remains protected, there is a vulnerability in the communication channels (specifically, the LPC bus) between the TPM and CPU during the boot-up phase. These channels lack encryption, making it possible for an attacker to intercept and access the insecurely encrypted encryption keys transmitted between the TPM and CPU.

On this hardware, the Youtuber successfully established a connection between a Raspberry Pi Pico and unutilized connectors on a test laptop. By doing so, he was able to extract the binary data during the machine's booting process. Within this extracted data, the Volume Master Key, stored on the TPM, was found. Consequently, this key allowed to decrypt additional data.

Affected products

Eviden is aware of this issue. Eviden does not use LPC Bus in its products.

Available Workarounds

No workaround is available.

Available Mitigations

The attack needs physical access to the motherboards which is usually prevented on Enterprise servers.

Available Exploits/PoC

The exploit only works with external TPMs that request data from the module using the LPC bus. Most modern hardware integrates the TPM. While a motherboard-based TPM could theoretically be exploited, it would require more time, effort, and an extensive period with the target device. Extracting BitLocker Volume Master Key data from a TPM becomes even more difficult if the module is integrated into the CPU.

Video with presented exploitation:

https://youtu.be/wTl4vEednkQ

References

1. https://youtu.be/wTl4vEednkQ
2. https://www.tomshardware.com/pc-components/cpus/youtuber-breaks-bitlocker-encryption-in-less-than-43-seconds-with-sub-dollar10-raspberry-pi-pico?utm_campaign=socialflow&utm_source=twitter.com&utm_medium=social
3. https://www.windowscentral.com/hardware/bitlocker-vulnerability-cracked-with-raspberry-pi-pico

Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information provides is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- https://support.bull.com/ols/product/security/psirt

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.