



[Full Disclosure](#) mailing list archives



◀ [By Date](#) ▶    ◀ [By Thread](#) ▶



## [SYSS-2022-015]: Verbatim Fingerprint Secure Portable Hard Drive - Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240) (CVE-2022-28382)

*From:* Matthias Deeg <matthias.deeg () syss de>

*Date:* Wed, 8 Jun 2022 16:02:12 +0200

Advisory ID:	SYSS-2022-015
Product:	Fingerprint Secure Portable Hard Drive
Manufacturer:	Verbatim
Affected Version(s):	#53650
Tested Version(s):	#53650
Vulnerability Type:	Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240)
Risk Level:	Low
Solution Status:	Open
Manufacturer Notification:	2022-02-03
Solution Date:	-
Public Disclosure:	2022-06-08
CVE Reference:	CVE-2022-28382
Author of Advisory:	Matthias Deeg (SySS GmbH)

~~~~~

### Overview:

The Verbatim Fingerprint Secure Portable Hard Drive is a USB drive with AES 256-bit hardware encryption and a built-in fingerprint sensor for unlocking the device with previously registered fingerprints.

The manufacturer describes the product as follows:

"The AES 256-bit Hardware Encryption seamlessly encrypts all data on the drive in real-time. The drive is compliant with GDPR requirements as 100% of the drive is securely encrypted. The built-in fingerprint recognition system allows access for up to eight authorised users and one administrator who can access the device via a password. The hard drive does not store passwords in the computer or system's volatile memory making it far more secure than software encryption." [1]

Due to the use of an insecure encryption AES mode (Electronic Codebook), an attacker may be able to extract information even from encrypted data, for example by observing repeating byte patterns.

~~~~~

## Vulnerability Details:

When analyzing the Verbatim Fingerprint Secure Portable Hard Drive, Matthias Deeg found out that the firmware of the USB-to-SATA bridge controller INIC-3637EN uses AES-256 with the ECB (Electronic Codebook) mode.

This operation mode of block ciphers like AES encrypts identical plaintext data, in this case blocks of 16 bytes, always to identical ciphertext data.

For some data, for instance bitmap images, the lack of the cryptographic property called diffusion concerning the ECB mode can leak sensitive information even in encrypted data.

One famous example for this is an ECB-encrypted image of the TUX penguin, which, for instance, is referenced in the Wikipedia article about block cipher modes of operation[2] to illustrate this issue.

Thus, the use of the ECB operation mode can put the confidentiality of specific information at risk, even in an encrypted form.

Additionally, in attack scenarios where an attacker has short-time physical access to a Verbatim Fingerprint Secure Portable Hard Drive, and later returns it to its legitimate owner, the attacker may be able to compromise the integrity of the stored data by exploiting the fact that the same 16-byte plaintext blocks result in the same 16-byte ciphertext blocks, by replacing specific encrypted 16-byte blocks with other ones.

~~~~~

## Proof of Concept (PoC):

The same 16 byte long plaintext pattern was written several times to an unlocked Verbatim Fingerprint Secure Portable Hard Drive.

When the hard drive was then read using another drive enclosure, the same 16 byte long ciphertext pattern could be observed for the corresponding plaintext data.

~~~~~

## Solution:

SySS GmbH is not aware of a solution for the described security issue.

~~~~~

## Disclosure Timeline:

2022-02-03: Vulnerability reported to manufacturer  
2022-02-11: Vulnerability reported to manufacturer again  
2022-03-07: Vulnerability reported to manufacturer again  
2022-06-08: Public release of security advisory

~~~~~

## References:

[1] Product website for Verbatim Fingerprint Secure Portable Hard Drive

<https://www.verbatim-europe.co.uk/en/prod/fingerprint-secure-portable-hard-drive-1tb-53650/>

[2] Wikipedia article about block cipher mode of operation

[https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation#Electronic\\_codebook](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook) (ECB)

[3] SySS Security Advisory SYSS-2022-015

<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-015.txt>

[4] SySS GmbH, SySS Responsible Disclosure Policy

<https://www.syss.de/en/responsible-disclosure-policy>

~~~~~

Credits:

This security vulnerability was found by Matthias Deeg of SySS GmbH.

E-Mail: matthias.deeg (at) syss.de

Public Key: [https://www.syss.de/fileadmin/dokumente/Materialien/PGPKeys/Matthias\\_Deeg.asc](https://www.syss.de/fileadmin/dokumente/Materialien/PGPKeys/Matthias_Deeg.asc)

Key fingerprint = D1F0 A035 F06C E675 CDB9 0514 D9A4 BF6A 34AD 4DAB

~~~~~

Disclaimer:

The information provided in this security advisory is provided "as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on the SySS website.

~~~~~

Copyright:

Creative Commons - Attribution (by) - Version 3.0

URL: <http://creativecommons.org/licenses/by/3.0/deed.en>

**Attachment:** [OpenPGP signature](#)

*Description:* OpenPGP digital signature

---

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <https://seclists.org/fulldisclosure/>

---

 [By Date](#)   [By Thread](#) 

## Current thread:

**[SYSS-2022-015]: Verbatim Fingerprint Secure Portable Hard Drive - Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240) (CVE-2022-28382) Matthias Deeg (Jun 10)**

Site Search



**Nmap Security Scanner**

Ref Guide

Install Guide

**Npcap packet capture**

User's Guide

API docs

**Security Lists**

Nmap Announce

Nmap Dev

**Security Tools**

Vuln scanners

Password audit

**About**

About/Contact

Privacy

Docs  
Download  
Nmap OEM

Download  
Npcap OEM

Full Disclosure  
Open Source Security  
BreachExchange

Web scanners  
Wireless  
Exploitation

Advertising  
Nmap Public Source  
License

