[SYSS-2022-002]: Verbatim Keypad Secure USB 3.2 Gen 1 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 15:30:39 +0200

```
Advisory ID:                SYSS-2022-002
Product:                    Keypad Secure USB 3.2 Gen 1 Drive
Manufacturer:               Verbatim
Affected Version(s):        Part Number #49428
Tested Version(s):          Part Number #49428
Vulnerability Type:         Use of a Cryptographic Primitive with a Risky
                            Implementation (CWE-1240)
Risk Level:                 Low
Solution Status:            Open
Manufacturer Notification:  2022-01-27
Solution Date:              -
Public Disclosure:          2022-06-08
CVE Reference:              CVE-2022-28382
Author of Advisory:         Matthias Deeg (SySS GmbH)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

The Verbatim Keypad Secure is a USB drive with AES 256-bit hardware
encryption and a built-in keypad for passcode entry.

The manufacturer describes the product as follows:

"The AES 256-bit Hardware Encryption seamlessly encrypts all data on the
drive in real-time with a built-in keypad for passcode input. The USB
Drive does not store passwords in the computer or system's volatile
memory making it far more secure than software encryption. Also, if it
falls into the wrong hands, the device will lock and require
re-formatting after 20 failed passcode attempts."[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 USB drive Verbatim Keypad Secure, 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 Keypad Secure USB 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 Keypad Secure USB drive.

When the SSD was then read using another SSD 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:

2022-01-27: 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 Keypad Secure

https://www.verbatim-europe.co.uk/en/prod/verbatim-keypad-secure-usb-32-gen-1-drive-64gb-49428/#
[2] Wikipedia article about block cipher mode of operation

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_(ECB)

[3] SySS Security Advisory SYSS-2022-002

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-002.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
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

By Date By Thread

Current thread:

[SYSS-2022-002]: Verbatim Keypad Secure USB 3.2 Gen 1 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
Docs

Npcap packet capture
User's Guide
API docs
Download

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure

Security Tools
Vuln scanners
Password audit
Web scanners

About
About/Contact
Privacy
Advertising
~~~~~~