Verbatim Store N Go Secure Portable HDD GD25LK01-3637-C VER4.0 Risky Crypto

Authored by Matthias Deeg | Site syss.de

Posted Jun 20, 2022

When analyzing the external SSD Verbatim Store 'n' Go Secure Portable HDD, 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.

tags | advisory
advisories | CVE-2022-28382
SHA-256 | 0a41b12ec159b56c4a817b283683266a073263b88ea74e74ebd6d5ec636346de Download | Favorite | View

Related Files

Share This

Change Mirror Download

```
Advisory ID:                SYSS-2022-006
Product:                    Store 'n' Go Secure Portable HDD
Manufacturer:               Verbatim
Affected Version(s):        GD25LK01-3637-C VER4.0
Tested Version(s):          GD25LK01-3637-C VER4.0
Vulnerability Type:         Use of a Cryptographic Primitive with a Risky
                             Implementation (CWE-1240)
Risk Level:                 Low
Solution Status:            Open
Manufacturer Notification: 2022-01-31
Solution Date:              -
Public Disclosure:          2022-06-08
CVE Reference:              CVE-2022-28382
Author of Advisory:         Matthias Deeg (SySS GmbH)

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

Overview:

The Verbatim Store 'n' Go Secure Portable HDD is a portable 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 password input. The SSD
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 SSD will lock and require re-formatting after
20 failed password 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 external SSD Verbatim Store 'n' Go Secure Portable
HDD, 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 Store 'n' Go Portable Secure HDD, 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.
```


File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

- Red Hat 186 files
- Ubuntu 52 files
- Gentoo 44 files
- Debian 27 files
- Apple 25 files
- Google Security Research 14 files
- malvuln 10 files
- nu11secur1ty 6 files
- mjurczyk 4 files
- George Tsimpidas 3 files

File Tags

- ActiveX (932)
- Advisory (79,557)
- Arbitrary (15,643)
- BBS (2,859)
- Bypass (1,615)
- CGI (1,015)
- Code Execution (6,913)
- Conference (672)
- Cracker (840)
- CSRF (3,288)
- DoS (22,541)
- Encryption (2,349)
- Exploit (50,293)
- File Inclusion (4,162)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

- AIX (426)
- Apple (1,926)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

The same 16 byte long plaintext pattern was written several times to an
unlocked Verbatim Store 'n' Go Secure Portable HDD.

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:

2022-01-31: 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 Store 'n' Go Secure Portable HDD

https://www.verbatim-europe.co.uk/en/prod/store-n-go-portable-ssd-with-keypad-access-256gb-53402/
[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-2022-006

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-006.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
```