Site Search

Full Disclosure mailing list archives

⬅ **By Date** ➡   ⬅ **By Thread** ➡

List Archive Search

[SYSS-2022-007]: Verbatim Store 'n' Go Secure Portable HDD - Missing Immutable Root of Trust in Hardware (CWE-1326) (CVE-2022-28383)

From: Matthias Deeg <matthias.deeg () syss de>
Date: Wed, 8 Jun 2022 15:53:35 +0200

```
Advisory ID:            SYSS-2022-007
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: Missing Immutable Root of Trust in Hardware (CWE-1326)
Risk Level:             Medium
Solution Status:        Open
Manufacturer Notification: 2022-01-31
Solution Date:          -
Public Disclosure:      2022-06-08
CVE Reference:          CVE-2022-28383
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 insufficient firmware validation, an attacker can store
malicious firmware code for the USB-to-SATA bridge controller on the
external drive which gets executed.


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

Vulnerability Details:

When analyzing the external SSD Verbatim Store 'n' Go Secure Portable
HDD, Matthias Deeg found out that the validation of the firmware for the
USB-to-SATA bridge controller INIC-3637EN only consists of a simple
CRC-16 check (XMODEM CRC-16).

Thus, an attacker is able to store malicious firmware code for the
INIC-3637EN with a correct checksum on the used SPI flash memory chip
(XT25F01D), which then gets successfully executed by the USB-to-SATA
bridge controller.

For instance, this security vulnerability could be exploited in a
so-called "supply chain attack" when the device is still on its way to
its legitimate user.

An attacker with temporary physical access during the supply could
program a modified firmware on the Verbatim Keypad Secure, which always
uses an attacker-controlled AES key for the data encryption, for
example.

If, later on, the attacker gains access to the used USB drive, he
can simply decrypt all contained user data.

~~~~~~

Proof of Concept (PoC):

SySS was able to read and write the SPI flash memory containing the
firmware of the INIC-3637EN controller (128 KB) using a universal
programmer.

By analyzing the dumped memory content, SySS found out that the
INIC-3637EN firmware is stored from the file offset 0x4000 to the file
offset 0x1BFFB, and that the corresponding XMODEM CRC-16 is stored at
the file offset 0x1FFFC.

Matthias Deeg developed a simple Python tool for updating the checksum
of modified firmware images before writing them to the SPI flash memory
chip.

The following output exemplarily shows updating a modified firmware
image:

```
$ python update-firmaware.py firmware_hacked.bin
Verbatim Store 'n' Go Firmware Updater v0.1 - Matthias Deeg, SySS GmbH (c) 2022
[*] Computed CRC-16 (0x03F5) does not match stored CRC-16 (0x8B17).
[*] Successfully updated firmware file
```

~~~~~~

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] SySS Security Advisory SYSS-2022-007

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-007.txt
[3] 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

_____
```
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-2022-007]: Verbatim Store 'n' Go Secure Portable HDD - Missing Immutable Root of Trust in Hardware (CWE-1326) (CVE-2022-28383) *Matthias Deeg (Jun 10)*

Site Search

Nmap Security Scanner   **Npcap packet capture**   **Security Lists**   **Security Tools**   **About**

Ref Guide

Install Guide

Docs

Download

Nmap OEM

User's Guide

API docs

Download

Npcap OEM

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About/Contact

Privacy

Advertising

Nmap Public Source License