[SYSS-2022-013]: Verbatim Executive Fingerprint Secure SSD - Insufficient Verification of Data Authenticity (CWE-345) (CVE-2022-28385)

From: Matthias Deeg <matthias.deeg () syss de>
Date: Wed, 8 Jun 2022 16:06:38 +0200

```
Advisory ID:               SYSS-2022-013
Product:                   Executive Fingerprint Secure SSD
Manufacturer:              Verbatim
Affected Version(s):       GDMSFE01-INI3637-C VER1.1
Tested Version(s):         GDMSFE01-INI3637-C VER1.1
Vulnerability Type: Insufficient Verification of Data Authenticity (CWE-345)
Risk Level:                Low
Solution Status:           Open
Manufacturer Notification: 2022-02-03
Solution Date:             -
Public Disclosure:         2022-06-08
CVE Reference:             CVE-2022-28385
Author of Advisory:        Matthias Deeg (SySS GmbH)

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

Overview:

The Verbatim Executive Fingerprint Secure SSD 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 SSD
does not store passwords in the computer or system's volatile memory
making it far more secure than software encryption."[1]

Due to missing integrity checks, an attacker can manipulate the content
of the emulated CD-ROM drive containing the Windows and macOS client
software.

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

Vulnerability Details:

When analyzing the Verbatim Executive Fingerprint Secure SSD, Matthias Deeg found out that the content of the emulated CD-ROM drive containing the Windows and macOS client software can be manipulated.

The content of this emulated CD-ROM drive is stored as ISO-9660 image in the "hidden" sectors of the USB drive that can only be accessed using special IOCTL commands, or when installing the drive in an external disk enclosure.

The following output exemplarily shows the content of the ISO-9660 file system:

```
# mount hidden_sectors.bin /mnt/

# lsd -laR /mnt/
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
drwxr-xr-x root root 4.0 KB Fri Jan  7 16:39:47 2022   ..
.r-xr-xr-x root root  70 B  Wed Aug 14 09:20:40 2019   Autorun.inf
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   MAC
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Windows

/mnt/MAC:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   setup.app
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Source

/mnt/MAC/setup.app:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Contents

/mnt/MAC/setup.app/Contents:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   _CodeSignature
.r-xr-xr-x root root 1.4 KB Thu Oct 24 06:58:18 2019   Info.plist
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   MacOS
.r-xr-xr-x root root   8 B  Thu Oct 24 06:58:18 2019   PkgInfo
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Resources

/mnt/MAC/setup.app/Contents/_CodeSignature:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root 3.6 KB Thu Oct 24 07:06:02 2019   CodeResources

/mnt/MAC/setup.app/Contents/MacOS:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root  30 KB Thu Oct 24 07:06:02 2019   setup

/mnt/MAC/setup.app/Contents/Resources:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Base.lproj

/mnt/MAC/setup.app/Contents/Resources/Base.lproj:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Main.storyboardc
```

```
/mnt/MAC/setup.app/Contents/Resources/Base.lproj/Main.storyboardc:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root 445 B  Thu Oct 24 06:58:18 2019   Info.plist
.r-xr-xr-x root root  35 KB Thu Oct 24 06:58:18 2019   MainMenu.nib
.r-xr-xr-x root root 3.5 KB Thu Oct 24 06:58:18 2019   NSWindowController-B8D-0N-5wS.nib
.r-xr-xr-x root root 1.2 KB Thu Oct 24 06:58:18 2019   XfG-lQ-9wD-view-m2S-Jp-Qdl.nib

/mnt/MAC/Source:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root 5.9 MB Mon Jul 22 06:22:24 2019   gtk_dylib.tar
.r-xr-xr-x root root 1.0 MB Thu Oct 24 07:23:30 2019   VERBATIM_FPTOOL_B0_V1.2.tar

/mnt/Windows:
r-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root 5.6 KB Fri Aug  9 10:47:26 2019   English.txt
.r-xr-xr-x root root 6.6 KB Fri Aug  9 10:47:26 2019   French.txt
.r-xr-xr-x root root 6.2 KB Fri Aug  9 10:47:26 2019   German.txt
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   Ico
.r-xr-xr-x root root 6.2 KB Fri Aug  9 10:47:26 2019   Italian.txt
.r-xr-xr-x root root 512 B  Fri Aug  9 10:47:26 2019   license.bin
.r-xr-xr-x root root 160 KB Fri Aug  9 10:47:26 2019   odbccp32.dll
.r-xr-xr-x root root 7.1 KB Fri Aug  9 10:47:26 2019   Spanish.txt
.r-xr-xr-x root root 4.9 MB Wed Apr  1 09:28:53 2020   VerbatimSecure.exe

/mnt/Windows/Ico:
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   .
dr-xr-xr-x root root 2.0 KB Wed Apr  1 09:29:50 2020   ..
.r-xr-xr-x root root  34 KB Fri Aug  9 10:47:26 2019   Verbatim.ico
```

By manipulating this ISO-9660 image or replacing it with another one, an attacker is able to store malicious software on the emulated CD-ROM drive which then may get executed by an unsuspecting victim when using the device.

For example, an attacker with temporary physical access during the supply could program a modified ISO-9660 image on the Verbatim Executive Fingerprint Secure SSD, which always uses an attacker-controlled password for unlocking the device.

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

Storing arbitrary other malicious software is also possible.

~~~~~~

Proof of Concept (PoC):

SySS could successfully modify the content of the ISO-9660 image containing the Windows and macOS software for unlocking and managing the Verbatim Executive Fingerprint Secure SSD.

~~~~~~

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 Executive Fingerprint Secure SSD

https://www.verbatim-europe.co.uk/en/prod/executive-fingerprint-secure-ssd-usb-32-gen-1--usb-c-1tb-53657/
[2] SySS Security Advisory SYSS-2022-013

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-013.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:

Attachment: **OpenPGP_signature**
Description: OpenPGP digital signature

By Date By Thread

Current thread:

- **[SYSS-2022-013]: Verbatim Executive Fingerprint Secure SSD - Insufficient Verification of Data Authenticity (CWE-345) (CVE-2022-28385)** *Matthias Deeg (Jun 10)*

Site Search

Nmap Security Scanner

- Ref Guide
- Install Guide
- Docs
- Download
- Nmap OEM

Npcap packet capture

- User's Guide
- API docs
- Download
- Npcap OEM

Security Lists

- Nmap Announce
- Nmap Dev
- Full Disclosure
- Open Source Security
- BreachExchange

Security Tools

- Vuln scanners
- Password audit
- Web scanners
- Wireless
- Exploitation

About

- About/Contact
- Privacy
- Advertising
- Nmap Public Source License