Verbatim Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1 Risky Crypto

Authored by Matthias Deeg | Site syss.de

Posted Jun 20, 2022

When analyzing the Verbatim Executive Fingerprint Secure SSD, Matthias Deeg found out it uses an insecure design which allows retrieving the currently used password and thus the ability to unlock and access the stored data in an unauthorized way.

tags | advisory
advisories | CVE-2022-28387
SHA-256 | 6d66162caa87e1410113575c6a6d6f93e01bfe781f0ffa5dbe090641a9dac682

Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Advisory ID:               SYSS-2022-009
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:        Use of a Cryptographic Primitive with a Risky
                            Implementation (CWE-1240)
Risk Level:                High
Solution Status:           Open
Manufacturer Notification: 2022-02-03
Solution Date:             -
Public Disclosure:         2022-06-08
CVE Reference:             CVE-2022-28387
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 an insecure design, the Verbatim Executive Fingerprint Secure SSD
can be unlocked by an attacker who can thus gain unauthorized access to
the stored data.

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

Vulnerability Details:

When analyzing the Verbatim Executive Fingerprint Secure SSD, Matthias
Deeg found out it uses an insecure design which allows retrieving the
currently used password and thus the ability to unlock and access the
stored data in an unauthorized way.

The Verbatim Executive Fingerprint Secure SSD consists of the following
five main parts:

1. An SSD in M.2 form factor
2. A USB-to-SATA bridge controller (INIC-3637EN)
3. An SPI flash memory chip (XT25F01D) containing the firmware of the
    INIC-3637EN
4. A fingerprint sensor
5. A fingerprint sensor controller (INIC-3782N)

For encrypting the data stored on the SSD, the hardware AES engine of
the INIC-3637EN is used. More specifically, AES-256 in ECB (Electronic
Codebook) mode is used for data encryption, which is also a security
issue by itself, as described in the SySS security advisory
SYSS-2022-010[2].

The SSD can be either unlocked via the fingerprint sensor using a
previously registered fingerprint or via a password.

Unlocking the SSD via a password takes place using a Windows or macOS
client software that sends specific IOCTL commands
(IOCTL_SCSI_PASS_THROUGH) to the USB device.
```

Follow us on Twitter

Subscribe to an RSS Feed

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)

```
The data part of those device-specific commands is encrypted using AES
with a hard-coded cryptographic key found within the client software
and the USB-to-SATA bridge controller's firmware.

One of the supported commands is able to retrieve the currently set
password and cryptographic key material used for the data disk
encryption.

By sending this specific IOCTL command to the USB device and knowing the
used AES encryption scheme for the command data, an attacker can
instantly retrieve the correct password and thus unlock the device in
order to gain unauthorized access to its stored data.

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

Proof of Concept (PoC):

For demonstrating the described security vulnerability, Matthias Deeg
developed a software tool that can extract the currently set password
of a Verbatim Executive Fingerprint Secure SSD. This enables an attacker
to instantly unlock the device.

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

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-2022-010

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-010.txt
[3] SySS Security Advisory SYSS-2022-009

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-009.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
```

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Login or Register to add favorites