

Verbatim Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1 Insufficient Verification

Authored by [Matthias Deeg](#) | Site [syss.de](#)

Posted Jun 20, 2022

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.

tags | [advisory](#)

systems | [windows](#)

advisories | [CVE-2022-28385](#)

SHA-256 | [26ff4e832d69529801ce9581fa340d311be8da080d073cf03ef28644ddb30a51](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror	Download
<p>Advisory ID: SYSS-2022-013</p> <p>Product: Executim Fingerprint Secure SSD</p> <p>Manufacturer: Verbatim</p> <p>Affected Version(s): GDMSFE01-INI3637-C VER1.1</p> <p>Tested Version(s): GDMSFE01-INI3637-C VER1.1</p> <p>Vulnerability Type: Insufficient Verification of Data</p> <p>Authenticity (CWE-345): Low</p> <p>Risk Level: Open</p> <p>Solution Status: 2022-02-03</p> <p>Manufacturer Notification: 2022-02-03</p> <p>Solution Date: -</p> <p>Public Disclosure: 2022-06-08</p> <p>CVE Reference: CVE-2022-28385</p> <p>Author of Advisory: Matthias Deeg (SySS GmbH)</p>	
<p>Overview:</p> <p>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.</p> <p>The manufacturer describes the product as follows:</p> <p>"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]</p> <p>Due to missing integrity checks, an attacker can manipulate the content of the emulated CD-ROM drive containing the Windows and macOS client software.</p>	
<p>Vulnerability Details:</p> <p>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.</p> <p>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.</p> <p>The following output exemplarily shows the content of the ISO-9660 file system:</p> <pre># mount hidden_sectors.bin /mnt/ # ls -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 ..</pre>	



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)

```
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-Qd1.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

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
PHP (5,087)	iOS (330)
Proof of Concept (2,290)	iPhone (108)
Protocol (3,426)	IRIX (220)
Python (1,449)	Juniper (67)
Remote (30,009)	Linux (44,118)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,768)	OpenBSD (479)
Shell (3,098)	RedHat (12,339)
Shellcode (1,204)	Slackware (941)
Sniffer (885)	Solaris (1,607)
Spoof (2,165)	SUSE (1,444)
SQL Injection (16,089)	Ubuntu (8,147)
TCP (2,377)	UNIX (9,150)
Trojan (685)	UnixWare (185)
UDP (875)	Windows (6,504)
Virus (661)	Other
Vulnerability (31,104)	
Web (9,329)	
Whitepaper (3,728)	
x86 (946)	
XSS (17,478)	
Other	

https://www.verbatim-europe.co.uk/en/prod/executive-fingerprint-secure-usb-32-gen-1--usb-c-ltb-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:

Creative Commons - Attribution (by) - Version 3.0

URL: <http://creativecommons.org/licenses/by/3.0/deed.en>

[Login](#) or [Register](#) to add favorites

**packet storm**

© 2022 Packet Storm. All rights reserved.

## Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

## About Us

[History & Purpose](#)

[Contact Information](#)

[Terms of Service](#)

[Privacy Statement](#)

[Copyright Information](#)

## Hosting By

[Rokasec](#)



Follow us on Twitter



Subscribe to an RSS Feed