

## Verbatim Keypad Secure USB 3.2 Gen 1 Drive Cryptography Issue

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

Posted Jun 19, 2022

When analyzing the USB drive Verbatim Keypad Secure version 3.2 Gen 1 Drive, Matthias Deeg found out it uses an insecure design which allows for offline brute-force attacks against the passcode.

tags | [advisory](#)

advisories | [CVE-2022-28384](#)

SHA-256 | [3ed883a011f776ec342336cc3c9cfdade67dfbd44f04b20239f15f16a6dc912e](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

[Like 0](#)

[Tweet](#)

[LinkedIn](#)

[Reddit](#)

[Digg](#)

[StumbleUpon](#)

### Change Mirror

### Download

Advisory ID: SYSS-2022-001  
Product: Keypad Secure USB 3.2 Gen 1 Drive  
Manufacturer: Verbatim  
Affected Version(s): Part Number #49428  
Tested Version(s): Part Number #49428  
Vulnerability Type: Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240)  
Risk Level: High  
Solution Status: Open  
Manufacturer Notification: 2022-01-27  
Solution Date: -  
Public Disclosure: 2022-06-08  
CVE Reference: CVE-2022-28384  
Author of Advisory: Matthias Deeg (SySS GmbH)

### Overview:

The Verbatim Keypad Secure is a 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 passcode input. The USB Drive 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 device will lock and require re-formatting after 20 failed passcode attempts."[1]

Due to an insecure design, the Verbatim Keypad Secure USB drive is vulnerable to an offline brute-force attack for finding out the correct passcode, and thus gaining unauthorized access to the stored encrypted data.

### Vulnerability Details:

When analyzing the USB drive Verbatim Keypad Secure, Matthias Deeg found out it uses an insecure design which allows for offline brute-force attacks against the passcode.

The Verbatim Keypad Secure consists of the following four main parts:

1. An SSD in M.2 form factor (SSD controller MARVELL-88NV1120)
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 keypad controller (unknown chip, marked "SW611 2121")

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 described in SySS security advisory SYSS-2022-002[2].

The cryptographic key for the actual data encryption, the so-called data encryption key (DEK), is stored in a special sector of the SSD which in turn is encrypted using AES-256-ECB with a so-called key encryption key (KEK).

This KEK is derived from the entered passcode which can be between five and twelve digits long, and can be generated by the keypad controller.

When the unlock button is pressed on the Verbatim Keypad Secure, this generated AES 256-bit key is transmitted via SPI communication from the keypad controller to the USB-to-SATA bridge controller INIC-3637EN for configuring the corresponding hardware AES engine.

For verifying the entered passcode, the firmware of the INIC-3637EN reads and decrypts the special sector on the SSD with the provided KEK, and checks specific data offsets for the known byte pattern (signature)



[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](#)

[mjrczyk 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 \(1,926\)](#)

"0x20 0x49 0x4E 0x49" which represents the string " INI".

If this byte pattern could successfully be found, the entered passcode and its derived AES key are very likely correct, and enable the firmware access to the decrypted DEK which can then be used to decrypt the actual SSD user data.

This described design of the Verbatim Keypad Secure allows for offline brute-force attacks for finding the correct passcode. Because an attacker can generate and observe the derived AES keys (KEK) of the keypad for all possible passcodes, and then try to correctly decrypt the data of the specific SSD sector. If the magic byte pattern " INI" can be found in the expected places of the resulting plaintext, the correct passcode was found, which then allows for gaining unauthorized access to the encrypted user data.

~~~~~

Proof of Concept (PoC):

For demonstrating the offline brute-force attack, Matthias Deeg developed a sample brute-forcing software tool which checks the complete search space of all possible passcodes between five and twelve digits.

~~~~~

Solution:

SySS GmbH is not aware of a solution for the described security issue.

~~~~~

Disclosure Timeline:

2022-01-27: 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 Keypad Secure  
<https://www.verbatim-europe.co.uk/en/prod/verbatim-keypad-secure-usb-32-gen-1-drive-64gb-49428/#>  
[2] SySS Security Advisory SYSS-2022-002  
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-002.txt>  
[3] SySS Security Advisory SYSS-2022-001  
<https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-001.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](mailto:matthias.deeg@syss.de)  
Public Key:  
[https://www.syss.de/fileadmin/dokumente/Materialien/PGPKeys/Matthias\\_Deeg.asc](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) | 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                     |                  |

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



© 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