Verbatim Keypad Secure USB 3.2 Gen 1 Drive Missing Control

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 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.

tags | advisory
advisories | CVE-2022-28383
SHA-256 | 52c1bd34c6801f46e1bba55d25c92e6597c84cbd41ec64b03d514cd0fa54e98f **Download** | **Favorite** | **View**

Related Files

Share This

Change Mirror Download

```
Advisory ID:                SYSS-2022-003
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:         Missing Immutable Root of Trust in Hardware
(CWE-1326)
Risk Level:                 Medium
Solution Status:            Open
Manufacturer Notification: 2022-01-27
Solution Date:              -
Public Disclosure:          2022-06-08
CVE Reference:              CVE-2022-28383
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 insufficient firmware validation, an attacker can store
malicious firmware code for the USB-to-SATA bridge controller on the USB
drive which gets executed.

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

Vulnerability Details:

When analyzing the USB drive Verbatim Keypad Secure, 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.
```


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)

```
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 Secure Keypad 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:

2022-01-27: 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] GitHub repository of flashrom
    https://github.com/flashrom/flashrom
[3] SySS Security Advisory SYSS-2022-003

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-003.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

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