Full Disclosure mailing list archives

By Date By Thread

List Archive Search

[SYSS-2022-024]: Lepin EP-KP001 - Violation of Secure Design Principles (CWE-657) (CVE-2022-29948)

From: Matthias Deeg <matthias.deeg () syss de>
Date: Fri, 10 Jun 2022 11:46:07 +0200

Advisory ID:	SYSS-2022-024
Product:	EP-KP001
Manufacturer:	Lepin
Affected Version(s):	KP001_V19
Tested Version(s):	KP001_V19
Vulnerability Type:	Violation of Secure Design Principles (CWE-657)
Risk Level:	High
Solution Status:	Open
Manufacturer Notification:	2022-04-12
Solution Date:	-
Public Disclosure:	2022-06-10
CVE Reference:	CVE-2022-29948
Author of Advisory:	Matthias Deeg (SySS GmbH)

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

Overview:

The Lepin EP-KP001 is a USB flash drive with AES-256 hardware encryption and a built-in keypad for passcode entry.

The manufacturer describes the product as follows (see [1]):

"[Safeguard Your Sensitive DATA] With Military Grade Full-disk 256-bit AES XTS Hardware Encryption to protect your important files. All your data is protected by hardware encryption, so no one can access your data without knowing the password."

Due to an insecure design, the Lepin EP-KP001 flash drive is vulnerable to an authentication bypass attack which enables an attacker to gain unauthorized access to the stored encrypted data.

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

Vulnerability Details:

When analyzing the USB flash drive Lepin EP-KP001, Matthias Deeg found out that it uses an insecure hardware design which allows an attacker to bypass the password-based user authentication.

The Lepin EP-KP001 consists of the following four main parts:

1. An unknown NAND flash memory chip
2. An Alcor Micro flash disk controller (AU6989SNBL-GTD)
3. An unknown microcontroller (unkmarked chip) used as keypad controller
4. A high-speed analog switch (SGM7222)

The encrypted disk partition with the stored user data can be unlocked by entering the correct passcode via the keypad and pressing the "unlock" button.

Due to the performed analysis, the password-based user authentication via a passcode comprised of 6 to 14 digits is performed by the unknown microcontroller.

By replacing this unknown microcontroller on a target device with one from an attacker-controlled Lepin EP-KP001 whose passcode was known, it was possible to successfully unlock the targeted Lepin EP-KP001 USB flash drive and to gain unauthorized access to the stored data in cleartext.

~~~~~~

Proof of Concept (PoC):

A successful authentication bypass attack could be performed via the following steps:

1. Set a passcode on an attacker-controlled Lepin EP-KP001.

2. Desolder the unmarked microcontroller from the attacker-controlled device.

3. Desolder the unmarked microcontroller from the targeted Lepin EP-KP001.

4. Solder the unmarked microcontroller from the attacker-controlled device on the targeted device.

5. Unlock the targeted device with the initially set and known passcode.

~~~~~~

Solution:

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

~~~~~~

Disclosure Timeline:

2022-04-12: Vulnerability reported to manufacturer
2022-06-10: Public release of security advisory

~~~~~~

References:

[1] Product website for Lepin EP-KP001

https://www.amazon.com/Encrypted-Password-Aluminum-Portable-Protected/dp/B06W5H9GP7/
[2] SySS Security Advisory SYSS-2022-024

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2022-024.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:

Attachment: OpenPGP_signature
Description: OpenPGP digital signature

By Date   By Thread

Current thread:

- **[SYSS-2022-024]: Lepin EP-KP001 - Violation of Secure Design Principles (CWE-657) (CVE-2022-29948)** ***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
~~~~~~