CVE-2023-25758

Published on: Not Yet Published

Last Modified on: 02/22/2023 04:15:00 PM UTC

CVE-2023-25758

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of Onekey Mini from Onekey contain the following vulnerability:

Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected."

CVE-2023-25758 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.2 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Our Response to Recent Security Fix Reports | by Masa | Feb, 2023 | OneKey	blog.onekey.so text/html	MISC blog.onekey.so/our-response-to-recent-security-fix-reports-13914fea8afd
GitHub - OneKeyHQ/firmware	github.com text/html	MISC github.com/OneKeyHQ/firmware
Cyber firm cracks OneKey crypto wallets, raises broader questions of hardware security | Fortune	fortune.com text/html	MISC fortune.com/crypto/2023/02/09/cyber-firm-cracks-onekey-crypto-wallets-in-video-raises-questions-hardware-security/amp/

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Onekey	Onekey Mini	-	All	All	All
Operating System	Onekey	Onekey Mini Firmware	All	All	All	All
Hardware	Onekey	Onekey Touch	-	All	All	All
Operating System	Onekey	Onekey Touch Firmware	All	All	All	All

cpe:2.3:h:onekey:onekey_mini:-:*:*:*:*:*:*:*:

cpe:2.3:o:onekey:onekey_mini_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:onekey:onekey_touch:-:*:*:*:*:*:*:*:

cpe:2.3:o:onekey:onekey_touch_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25758 : Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle… twitter.com/i/web/status/1…	2023-02-14 07:03:16
/r/netcve	CVE-2023-25758	2023-02-14 08:38:42

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report