



CVE-2019-14353

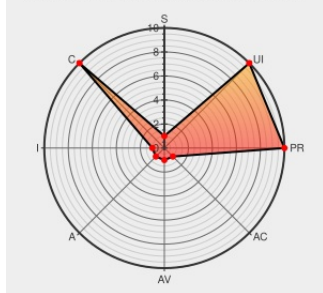
Published on: 08/08/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-14353

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [One](#) from [Trezor](#) contain the following vulnerability:

On Trezor One devices before 1.8.2, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. In other

words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data. NOTE: this CVE applies exclusively to the Trezor One, and does not refer to any issues with OLED displays on other devices.

CVE-2019-14353 has been assigned by [M](#) 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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Details of the OLED Vulnerability and its Mitigation by SatoshiLabs Trezor Blog	Exploit Mitigation Third Party Advisory blog.trezor.io text/html	MISC blog.trezor.io/details-of-the-oled-vulnerability-and-its-mitigation-d331c4e2001a

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Trezor	One	-	All	All	All
Hardware 	Trezor	One	-	All	All	All
Operating System	Trezor	One Firmware	All	All	All	All
Operating System	Trezor	One Firmware	All	All	All	All
cpe:2.3:h:trezor:one:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:trezor:one:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:trezor:one_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:trezor:one_firmware:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)