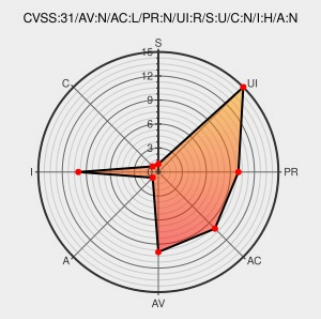
CVE-2020-14199

Published on: 06/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-14199

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



Certain versions of Trezor Model T from Satoshilabs contain the following vulnerability:

BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T.

CVE-2020-14199 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Details of firmware updates for Trezor One (version 1.9.1) and Trezor Model T (version 2.3.1) | by Pavol Rusnak | Trezor Blog	Third Party Advisory, blog.trezor.io, text/html	MISC blog.trezor.io/details-of-firmware-updates-for-trezor-one-version-1-9-1-and-trezor-model-t-version-2-3-1-1eba8f60f2dd

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	Satoshilabs	Trezor Model T	-	All	All	All
Hardware	Satoshilabs	Trezor Model T	-	All	All	All
Operating System	Satoshilabs	Trezor Model T Firmware	All	All	All	All
Operating System	Satoshilabs	Trezor Model T Firmware	All	All	All	All
Hardware	Satoshilabs	Trezor One	-	All	All	All
Hardware	Satoshilabs	Trezor One	-	All	All	All
Operating System	Satoshilabs	Trezor One Firmware	All	All	All	All
Operating System	Satoshilabs	Trezor One Firmware	All	All	All	All

cpe:2.3:h:satoshilabs:trezor_model_t:-:*:*:*:*:*:*:*:

cpe:2.3:h:satoshilabs:trezor_model_t:-:*:*:*:*:*:*:*:

cpe:2.3:o:satoshilabs:trezor_model_t_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:satoshilabs:trezor_model_t_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:satoshilabs:trezor_one:-:*:*:*:*:*:*:*:

cpe:2.3:h:satoshilabs:trezor_one:-:*:*:*:*:*:*:*:

cpe:2.3:o:satoshilabs:trezor_one_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:satoshilabs:trezor_one_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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