Fix side-channel in BIP-39 mnemonic processing when unlocked

Reported on September 24, 2025

Please note that the following attack is possible only in case the attacker has the Trezor in **physical possession** and the device is in an **unlocked** state. In such cases, the attacker can also simply send the funds right away.

In earlier firmware versions of Trezor Model One, the function mnemonic_to_bits() was called to check the recovery seed integrity after Trezor was unlocked. This function was not constant-time and could lead to seed extraction by an attacker who was in physical possession of the unlocked device.

This has been fixed by removing the integrity check, which was redundant, because there is another, even stronger, integrity check already in place.

In earlier universal firmware versions of Trezor Model T, Safe 3 and Safe 5 the same function could be used after Trezor was unlocked to convert the BIP-39 recovery seed to binary form which is needed to derive particular keys.

This has been fixed by storing a binary copy of the BIP-39 recovery seed. The vulnerable function was also fixed by replacing binary search over the wordlist with a linear search to ensure the same number of comparisons.

As mentioned at the beginning, the attacker can also simply send the funds right away. Nevertheless, it is a violation of our threat model where Trezor displays the backup only once.

This attack concerns all Trezor One devices. It also concerns Trezor Model T, Safe 3 and Safe 5 running universal firmware with BIP-39 backup. It doesn't concern Trezor Safe 7 and it doesn't concern Model T, Safe 3 or Safe 5 that are either running bitcoin-only firmware or use SLIP-39 backup, which is the default on these devices.

Resolved

Reported by Jiwoo Baek & HeeSeok Kim

Trezor Safe 3, Trezor Safe 5

Resolved vulnerabilities

Reported by the community. Investigated. Resolved. Because your security is never optional.

Reflected cross-site scripting (XSS) vulnerability on connect.trezor.io via hash fragment script injection
March 25, 2026

Open redirect on affiliate page
March 20, 2026

Biometric Verification bypassed in Trezor Suite with external monitor
March 9, 2026

Insufficient entropy on Trezor Model One with 12/18 words
February 6, 2026

Bug in multisig verification
January 10, 2026

Inability to cancel certain flows on pre-production firmware
October 31, 2025

Load more

TREZOR

a part of SatoshiLabs Group.

Products +

App

Coins

Learn +

Other +