BTCX Comments on the Troubles with Bitcoin theft from ColdCard - The Bitcoin protocol itself has not been hacked

"This is not a pleasant event for the Bitcoin community, but it's important to know that nothing is wrong with the Bitcoin network itself — it's a single provider that has failed to meet the required standard. As one of the oldest operators in Europe and the world, BTCX is keen to come forward with information about what has happened and what one should do if you are using the affected service. Customers can reach out to BTCX support with any questions, and for our OTC clients, we're launching a dedicated service in just a couple of weeks focused on both physical and digital security," says Christian Ander, CEO of Goobit Group AB.

In short: If you generated a seed phrase on a Coldcard device, act now and move your bitcoin. A "seed" is, in practice, your 12 words, and in this case the problem is that they have been more predictable than usual, even though everything looks normal on the surface — read on for technical details.

A critical entropy failure in Coldcard hardware wallets has been disclosed. Unlike the collapses of Mt. Gox, Quadriga, or FTX, this incident did not involve an exchange or trading venue. It affected users who followed best practices by generating their own keys on a hardware device that many in the industry had long recommended as a secure option for self-custody. As of now, approximately 594 BTC has been stolen from roughly 500 affected wallets.
Bitcoin's underlying cryptography remains intact. The problem was in the seed-generation process on certain Coldcard firmwares, which in some cases produced seeds with far less entropy than intended — in some cases as low as 40–72 bits instead of the intended 128. Low-entropy seeds are not visually distinguishable from secure ones until they are exploited.

Our position
BTCX has never recommended or promoted Coldcard devices. We have exclusively directed customers toward Trezor hardware wallets. Security is a continuously moving target. For any meaningful amount of bitcoin we continue to recommend diversified setups — different hardware vendors, multisignature configurations, and strong external entropy or passphrases where appropriate. Note that a multisignature setup built entirely from affected Coldcard devices does not provide protection; at least one key must come from an unaffected source.

Immediate action required
According to the manufacturer's current security advisory, the issue affects seeds generated under the following
conditions:
- Coldcard Mk2 or Mk3 running firmware versions 4.0.1 through 4.1.9
- Coldcard Mk4 or Mk5 before standard firmware version 5.6.0

- Coldcard Mk4 or Mk5 before Edge firmware version 6.6.0X
- Coldcard Q before standard firmware version 1.5.0Q
- Coldcard Q before Edge firmware version 6.6.0QX
- Do not wait

Move your bitcoin now.
Use a high fee so your transaction is unlikely to be displaced by a replace-by-fee attempt from an attacker who may already be monitoring or racing the same UTXOs. Take a moment to carefully verify the receiving address before sending — in a time-sensitive situation, a rushed or mistyped transfer is itself a common cause of lost funds.
Updating your device's firmware does not repair an already-compromised seed. Funds must be actively moved to a new, securely generated wallet.
Once the funds are moved to a secure new setup, you can take the time to build a more robust long-term custody arrangement. Do not leave significant value on any single-signature seed that was generated under the vulnerable conditions.

Going forward
This event is a reminder that no single device or vendor is a permanent guarantee. Review your own setup. Prefer multisignature with keys generated on independent devices from different manufacturers. Verify entropy sources. Keep your recovery processes tested and private.
We are monitoring the situation closely and will issue further updates if new information becomes available. If you have questions about migrating from an affected device, verifying whether your setup is at risk, or strengthening your current setup, contact support through the usual channels — we're here to help, and it's always better to ask than to guess.

For further information, please contact:
Christian Ander, CEO, Goobit Group AB

Email: ir@goobit.se

About Goobit Group | BTCX
Goobit Group AB (publ) operates within the financial sector and launched BTCX in 2011—the world's first still-operating bitcoin-only exchange. Goobit is Sweden's leading bitcoin company in financial services and education. The Group offers exchange services from fiat currencies to bitcoin. Its most well-known brands are BTCX Express Exchange, Standard Exchange (BTCX), OTC Exchange and Bitcoin Treasury. Goobit Group AB (publ) was registered in 2013 and consists of the wholly owned subsidiaries Goobit AB and Goobit Blocktech AB. The Group is headquartered in Stockholm, Sweden.

Attachments

BTCX Comments on the Troubles with Bitcoin theft from ColdCard - The Bitcoin protocol itself has not been hacked