

Forum:[Hack Forums](#)

Thread: [594 BTC Stolen from Hardware Wallet Coldcard](#)

Omniscient - July 31, 2026, 8:40 am

This is making the headlines this morning.

It would seem AI helped cracked their hardware wallet (Coldcard). Over 400 wallets drained in less than 30 minutes. Over \$38m dollars. And this is an air-gapped hardware wallet.

The current accusation is that AI found a firmware bug for the wallet in version Mk3. The wallet made easy to replicate seeds.

Not a good day for about 500 people.

Mewtwo - July 31, 2026, 8:47 am

Makes me worried about Trezor and other crypto hardware wallets. I'd probably just stick to my own random generated seed from an offline computer

DramaKing - July 31, 2026, 8:50 am

How is cracking a cold wallet remotely possible?

Motusora - July 31, 2026, 8:53 am

so , are they gonna refund those users ?

Omniscient - July 31, 2026, 8:56 am

(Jul 31, 2026 08:50 AM)DramaKing Wrote: [\[CITE\]](#) How is cracking a cold wallet remotely possible? The rumor is that the way the seed was formed was guessable. The randomness of the seed creation was garbage.

I'd be so livid right now if I list my BTC because of a "secure" air-gapped hardware wallet.

campusminger - July 31, 2026, 8:56 am

this is nightmare.
makes you question all hw wallets in market.

Shapeless - July 31, 2026, 9:03 am

Sick< i wish it was me that ran into that find lol :D

Well done to whoever did this if they dont need the change throw it this way wont ya ? :)

bc1q9fv7lvqhdjzut26077st8dgpecumjupavgch9u

DramaKing - July 31, 2026, 10:24 am

(Jul 31, 2026 08:56 AM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the way the seed was formed was guessable. The randomness of the seed creation was garbage.

I'd be so livid right now if I list my BTC because of a "secure" air-gapped hardware wallet. One seed for 400 wallets? I guess that I'd have to understand how it works.

Omniscient - July 31, 2026, 10:35 am

(Jul 31, 2026 10:24 AM)DramaKing Wrote: [\[CITE\]](#) One seed for 400 wallets? I guess that I'd have to understand how it works.

I'm not sure a single seed was generated for multiple wallets. If that was the case then someone with a wallet would have seen one giant balance that wasn't theirs.

Maybe this guys explanation will help.

bebonzy09 - July 31, 2026, 12:01 pm

This is shocking tbh and I never once trusted hardware wallets. I use an air gapped laptop whenever I need to sign or access my funds with electrum, its harder and harder to trust these wallets... Ledger and trezor both had databreaches and issues in the past too.

SIM-2470866 - July 31, 2026, 12:12 pm

cant wait for a case-study from ZachXBT on this.

Mewtwo - July 31, 2026, 12:42 pm

(Jul 31, 2026 12:12 PM)SIM-2470866 Wrote: [\[CITE\]](#) cant wait for a case-study from ZachXBT on this.

They're not paying him to investigate so most likely he doesn't care

Costanza - July 31, 2026, 12:56 pm

LOL poor crypto can't catch a break but yeah more hacking will happen and the price will continue to go down. no surprise

SUI-3183372 - July 31, 2026, 2:19 pm

Lot of rumors flying around on this one. First and foremost, Coldcard did not roll their own crypto, it uses standard secp256k1/BIP39.

What happened was they unintentionally crippled their implementation of secp256k1/BIP39 back in a 2021 update. The update changed the seed generation call so that it bypassed the STM32 hardware random number generator and fell through to a weak software fallback. This fallback was seeded from a predictable combination of the device's serial number and its internal clock. This resulted in the entropy feeding the standard deterministic derivation was guessable and a much narrower set of possibilities than what it should have been.

This is where it got interesting for me, I was wondering how an attacker would be able to identify a Coldcard wallet on chain and look to compromise it, when the approach is actually far easier and far more efficient. From here, the attacker:

Enumerate the plausible serial number/clock combinations that the broken RNG could have used.

Run each through that same broken path to achieve the BIP32 master key

Derive address sets from from each master key

Check addresses against the chain, drain any that hold value.

Essentially, the number of combinations of serial numbers and times created a tiny enough landscape that an attacker can simply generate wallets for every single combination that can exist, and then check which of those hold a balance, and drain them. This likely resulted in millions if not tens of millions if not hundreds of millions of wallets generated, and they probably spent a considerable amount of time mapping which had funds. This resulted in 4 billion to 1 trillion of seeds generated, and once they sufficiently mapped their total address set containing funds, they would have struck them all at once.

This is structurally the same exploit as Milk Sad from 2023 and Randstorm from earlier in Bitcoin's life.

Omniscient - July 31, 2026, 2:34 pm

(Jul 31, 2026 02:19 PM)SUI-3183372 Wrote: [\[CITE\]](#) Lot of rumors flying around on this one. First and foremost, Coldcard did not roll their own crypto, it uses standard secp256k1/BIP39.

What happened was they unintentionally crippled their implementation of secp256k1/BIP39 back in a 2021 update. The update changed the seed generation call so that it bypassed the STM32 hardware random number generator and fell through to a weak software fallback. This fallback was seeded from a predictable combination of the device's serial number and its internal clock. This resulted in the entropy feeding the standard deterministic derivation was guessable and a much narrower set of possibilities than what it should have been.

This is where it got interesting for me, I was wondering how an attacker would be able to identify a Coldcard wallet on chain and look to compromise it, when the approach is actually far easier and far more efficient. From here, the attacker:

Enumerate the plausible serial number/clock combinations that the broken RNG could have used.

Run each through that same broken path to achieve the BIP32 master key

Derive address sets from from each master key

Check addresses against the chain, drain any that hold value.

Essentially, the number of combinations of serial numbers and times created a tiny enough landscape that an attacker can simply generate wallets for every single combination that can exist, and then check which of those hold a balance, and drain them. This likely resulted in millions if not tens of millions if not hundreds of millions of wallets generated, and they probably spent a considerable amount of time mapping which had funds, and once they sufficiently mapped their total address set, they would have struck them all at once (This is speculation on my behalf).

This is structurally the same exploit as Milk Sad from 2023 and Randstorm from earlier in Bitcoin's life.

Do you think the attacker had this exploit running against address for months or years before actually draining wallets? Seem to me that running that many combinations would take a lot of time. Assume the attacker once they found the exploit wanted to maximize the theft.

I also think it's odd they moved all the BTC into a few addresses. Less addresses are much easier to track and block.

bc1qq85v2c926eg6pgxhwp6q7lf6cnsz80qs3fcu9r (562 BTC)

bc1qx76cae2706qd5q576feh7xq8rfcsjpf2htfhe3 (398 BTC)

SUI-3183372 - July 31, 2026, 3:24 pm

(Jul 31, 2026 02:34 PM)Omniscient Wrote: [\[CITE\]](#) Do you think the attacker had this exploit running against address for months or years before actually draining wallets? Seem to me that running that many combinations would take a lot of time. Assume the attacker once they found the exploit wanted to maximize the theft.

I also think it's odd they moved all the BTC into a few addresses. Less addresses are much easier to track and block.

bc1qq85v2c926eg6pgxhwp6q7lf6cnsz80qs3fcu9r (562 BTC)

bc1qx76cae2706qd5q576feh7xq8rfcsjpf2htfhe3 (398 BTC)

Hard to say without understanding the full seed space. Per The Block, they're estimating this seed space was roughly 2^{32} (4.3 billion) seeds. Coinkite argues against The Block's claims, with an argument that effectively boils down to the seed space being somewhere between 2^{32} and 2^{40} (4.3 billion to roughly 1 trillion) seeds. This is much higher than I estimated in my last post, but still a trivially low number.

Theoretically each seed can have many addresses that hold funds, I'm uncertain if the attacker checked many addresses, or just the address at index 0. I'd probably only check index 0, at first pass, and then check for additional addresses pertaining to any seed that had an active address at index 0.

Lets assume the 2^{32} number is correct, then a sufficiently thorough attack would result in a seed space of 4.3 billion seeds checking 4.3 billion addresses sitting in index 0. If the attacker is a Hackforums user sitting at home with a 4090, then they pulled it off in no more than 12 hours, potentially as low as just 2-3 hours. An attacker with more resources could pull it off in 10 minutes.

If the 2^{40} number is more correct, then just multiple the above times by 20x-25x.

Basically anyone with a gaming PC and an open Friday night could have pulled this off. Any of you here responsible? ?

(Jul 31, 2026 02:34 PM)Omniscient Wrote: [\[CITE\]](#) I also think it's odd they moved all the BTC into a few addresses. Less addresses are much easier to track and block.

bc1qq85v2c926eg6pgxhwp6q7lf6cnsz80qs3fcu9r (562 BTC)

bc1qx76cae2706qd5q576feh7xq8rfcsjpf2htfhe3 (398 BTC)

Lazarus group have proven that consolidating your stolen funds ON BITCOIN results in no real hardship for them. If you were pulling off smaller thefts and trying to fly below the radar, sure, keeping things fanned out is probably for the best, but a theft as big as this you were going to have a lot of eyes on you anyway. I'd just follow the north korean playbook:

1. Consolidate funds (This step may swap with step 2 depending on what chain and bridges you need to use)
2. Move funds to BTC as quickly as possible assuming they aren't already
3. Go dormant for a few years

4. Launder aggressively once the heat dies down / dear leader asks for money

Omniscient - July 31, 2026, 3:36 pm

(Jul 31, 2026 03:24 PM)SUI-3183372 Wrote: [\[CITE\]](#) Hard to say without understanding the full seed space. Per The Block, they're estimating this seed space was roughly 2^{32} (4.3 billion) seeds. Coinkite argues against The Block's claims, with an argument that effectively boils down to the seed space being somewhere between 2^{32} and 2^{40} (4.3 billion to roughly 1 trillion) seeds. This is much higher than I estimated in my last post, but still a trivially low number.

Theoretically each seed can have many addresses that hold funds, I'm uncertain if the attacker checked many addresses, or just the address at index 0. I'd probably only check index 0, at first pass, and then check for additional addresses pertaining to any seed that had an active address at index 0.

Lets assume the 2^{32} number is correct, then a sufficiently thorough attack would result in a seed space of 4.3 billion seeds checking 4.3 billion addresses sitting in index 0. If the attacker is a Hackforums user sitting at home with a 4090, then they pulled it off in no more than 12 hours, potentially as low as just 2-3 hours. An attacker with more resources could pull it off in 10 minutes.

If the 2^{40} number is more correct, then just multiple the above times by 20x-25x.

Lazarus group have proven that consolidating your stolen funds ON BITCOIN results in no real hardship for them. If you were pulling off smaller thefts and trying to fly below the radar, sure, keeping things fanned out is probably for the best, but a theft as big as this you were going to have a lot of eyes on you anyway. I'd just follow the north korean playbook:

1. Consolidate funds (This step may swap with step 2 depending on what chain and bridges you need to use)
2. Move funds to BTC as quickly as possible assuming they aren't already
3. Go dormant for a few years
4. Launder aggressively once the heat dies down / dear leader asks for money

I'm wondering for obfuscation if doing a higher index like 15 on a new wallet might help protect against drainers. I gotta assume most of the time they don't go very deep.

Zexo - July 31, 2026, 3:40 pm

(Jul 31, 2026 09:03 AM)Shapeless Wrote: [\[CITE\]](#) Sick< i wish it was me that ran into that find lol :D

Well done to whoever did this if they dont need the change throw it this way wont ya ? :)

bc1q9fv7lvqhdjzut26077st8dgpecumjupavgch9u
You'd be getting a knock on your door.

SUI-3183372 - July 31, 2026, 4:12 pm

(Jul 31, 2026 03:36 PM)Omniscient Wrote: [\[CITE\]](#) I'm wondering for obfuscation if doing a higher index like 15 on a new wallet might help protect against drainers. I gotta assume most of the time they don't go very deep.

It could definitely save you. Use index 495, I'm certain there are scenarios where someone checks just index 0 or the first ~20 or so.

Your seed is still compromised, and thus should be considered burnt, but at least it may save you in a large scale attack that's not checking all indexes of all seeds.

Omniscient - July 31, 2026, 4:31 pm

(Jul 31, 2026 04:12 PM)SUI-3183372 Wrote: [\[CITE\]](#) It could definitely save you. Use index 495, I'm certain there are scenarios where someone checks just index 0 or the first ~20 or so.

Your seed is still compromised, and thus should be considered burnt, but at least it may save you in a large scale attack that's not checking all indexes of all seeds.

Should at least buy you some time.

I just found out a local buddy of mine with a very reasonable BTC sum had used the Coldcard wallet. He says he didn't lose anything but he's scrambling to rebuild his storage right now.

ModernEHustle - July 31, 2026, 4:41 pm

AI is making being a black hat much easier.

I wonder if it's going to be another Malone situation.

SUI-3183372 - July 31, 2026, 5:46 pm

(Jul 31, 2026 04:31 PM)Omniscient Wrote: [\[CITE\]](#) Should at least buy you some time.

I just found out a local buddy of mine with a very reasonable BTC sum had used the Coldcard wallet. He says he didn't lose anything but he's scrambling to rebuild his storage right now.

This only impacted a subset of Coldcard users.

Any seed generated before March 2021 is safe.

If you added a sufficient amount of additional entropy while generating, you're safe.

If you opted in to BIP-39's 25th word (passphrase), you're safe.

Devices Mk4, Mk5, and Q seem to be vulnerable, but at a 2^{72} vulnerable seed landscape vs mk2 and mk3's 2^{32} vulnerable seed landscape.

Jahad - July 31, 2026, 8:34 pm

Oh wow, I thought the whole point of physical hardware wallets was to make sure this kind of stuff doesn't happen.

NoodleBot™ - August 1, 2026, 12:41 am

(Jul 31, 2026 08:34 PM)Jahad Wrote: [\[CITE\]](#) Oh wow, I thought the whole point of physical hardware wallets was to make sure this kind of stuff doesn't happen.

It is. But as developers they failed to add the appropriate RNG kind of think of it as a video game where RNG matters like perhaps Pokémon wild encounters or damage in an RPG. There is an element of randomness applied, which requires entropy which is very difficult for humans to do so we rely on specific math for this entropy to work.

If you cheap out and do the lazy route on the math, you're gonna get entropy, but it's kind of predictable and it's replicated by other people that are trying to do the same thing. You'll end up with the same results over and over again time after time eventually.

TLDR they took the easy way out. There's tonnes of ways to explain proper entropy and RNG but I'm half retarded so you're not gonna get that fully out of me.

Here's something from Coldcard owners site tho

-not my stuff below from Coinkite websites-

“Updated July 31, 2026 at 12:39 p.m. EDT: Fixed firmware is now available for every affected model and release track:

Mk3: version 4.2.0 or later

Mk4/Mk5 standard: version 5.6.0 or later

Q standard: version 1.5.0Q or later

Mk4/Mk5 Edge: version 6.6.0X or later

Q Edge: version 6.6.0QX or later

Standard and Edge are separate release tracks. If you use Edge, install the fixed Edge release for your model. Do not assume an older Edge 6.x release is fixed merely because its version number is higher than the standard release.

Do not generate a new seed on any of these models until the update is installed.

Coinkite is warning all users who generated a seed using a Mk3 on version 4.0.1 (March 2021) thru 4.1.9 (inclusive) that their funds may be at risk.

Seeds generated on Mk4, Q and Mk5 before the fixed firmware releases are also affected, with about 72 bits of entropy rather than the expected 128 bits.

Updating the firmware does not change or repair an existing seed. If your seed was generated before the fixed firmware version for your model, follow the migration guidance below unless the independent dice-entropy exception applies to you.

TAPSIGNER, OPENDIME and SATSCARD are not affected by this bug as they are different codebases

The issue is present on Mk3 firmware versions 4.0.1 through 4.1.9 inclusive. It also affects seeds generated on Mk4 and Mk5 before standard version 5.6.0 or Edge version 6.6.0X, and on Q before standard version 1.5.0Q or Edge version 6.6.0QX. The impact on Mk4, Mk5 and Q is not as severe but is still serious.

If You Added Dice When Creating the Seed

This issue affects the device-generated entropy. It does not remove independent entropy that you supplied with dice.

On affected firmware, COLDCARD hashed the device-generated seed together with every dice roll entered through Add Dice Rolls:

50 to 98 independent, private rolls: the dice input alone contributed at least 128 bits of entropy.

99 or more independent, private rolls: the dice input contributed approximately 256 bits of entropy.

Fewer than 50 rolls, or you do not remember: follow the migration guidance in this advisory.

If you entered at least 50 fair and independent rolls, and the rolls were not recorded or exposed, we do not consider the resulting seed at risk from this RNG issue alone.

This applies to the final seed words shown after the dice were added. If you are uncertain which words you used, how many rolls you entered, or whether the rolls were private, migrate to a new seed.”

(Jul 31, 2026 05:46 PM)SUI-3183372 Wrote: [\[CITE\]](#) This only impacted a subset of Coldcard users.

Any seed generated before March 2021 is safe.

If you added a sufficient amount of additional entropy while generating, you're safe.

If you opted in to BIP-39's 25th word (passphrase), you're safe.

Devices Mk4, Mk5, and Q seem to be vulnerable, but at a 2^{72} vulnerable seed landscape vs mk2 and mk3's 2^{32} vulnerable seed landscape.

Do you think AI found this? Or did someone planted this out secretly from their internal side?

If it's AI, I'm sure there's going to be a lot of logs and traces back to that. How likely can an AI company be sued for finding a bug that allowed someone to steal this amount?

I'm sure stuff like this is going to push politicians to be more stricter on the cybercrime aspect. Punish the companies for facilitating a crime like an accomplice if no proper safeguards and verifications are in place.

Shapeless - August 1, 2026, 5:44 am

(Jul 31, 2026 03:40 PM)Zexo Wrote: [\[CITE\]](#) You'd be getting a knock on your door.

Hehe not where I am, I am in islamic republic probably would get a thank j card.

SUI-3183372 - August 1, 2026, 8:36 am

(Aug 1, 2026 04:17 AM)Mewtwo Wrote: [\[CITE\]](#) Do you think AI found this? Or did someone planted this out secretly from their internal side?

If it's AI, I'm sure there's going to be a lot of logs and traces back to that. How likely can an AI company be sued for finding a bug that allowed someone to steal this amount?

I'm sure stuff like this is going to push politicians to be more stricter on the cybercrime aspect. Punish the companies for facilitating a crime like an accomplice if no proper safeguards and verifications are in place.

I imagine it's very likely that AI played a role.

Likely identified the March 2021 update that weakened their crypto. Likely identified the manner in which it could be exploited. Using Kimi, it may have even written the exploit code for them.

Three - August 1, 2026, 8:57 am

The mistake made by the individuals whose BTC was stolen was using only a single hardware wallet. Holders of large amounts of BTC should use two different hardware wallets.

Someone on Reddit had 0.8 BTC stolen; that's a lot of money.

For example, the Ledger Nano S Plus is 70 USD. Trezor Safe 3 50 USD...

I am not saying these are bug-free or completely secure. At the very least, if an error occurs, your entire cryptocurrency holdings won't vanish. It is impossible for your funds to be stolen from both hardware wallets simultaneously.

SUI-3183372 - August 1, 2026, 9:05 am

Your BTC key is just fancy cryptography that can be replicated anywhere, you don't need a wallet provider or any third party to generate a valid BTC keypair and address.

1. Set up local / air gapped environment to generate BTC keypair
2. Generate your own keypair

3. Never connect this keypair to any hardware or software wallets
4. Send funds intended for cold storage to address
5. Store key in a KeePass database (local encrypted pw manager)
6. Store database on numerous USB drives
7. Store USB drives in safe locations

If someone finds a USB, they won't be able to decrypt your database assuming you've chosen a sufficient pass phrase.

Omniscient - August 1, 2026, 10:03 am

(Aug 1, 2026 09:05 AM)SUI-3183372 Wrote: [\[CITE\]](#) Your BTC key is just fancy cryptography that can be replicated anywhere, you don't need a wallet provider or any third party to generate a valid BTC keypair and address.

1. Set up local / air gapped environment to generate BTC keypair
2. Generate your own keypair
3. Never connect this keypair to any hardware or software wallets
4. Send funds intended for cold storage to address
5. Store key in a KeePass database (local encrypted pw manager)
6. Store database on numerous USB drives
7. Store USB drives in safe locations

If someone finds a USB, they won't be able to decrypt your database assuming you've chosen a sufficient pass phrase.

Correct.

Hardware wallets aren't all that fancy imho.

And using encrypted USB drives is one method I personally use.

Costanza - August 1, 2026, 12:37 pm

(Jul 31, 2026 08:34 PM)Jahad Wrote: [\[CITE\]](#) Oh wow, I thought the whole point of physical hardware wallets was to make sure this kind of stuff doesn't happen.

Will continue to happen as AI will keep hacking them LOL.

Crypto is done and people are yet to see it

bebonzy09 - August 2, 2026, 7:07 pm

You know what I've been thinking the last few days, why didn't the attacker just sweep a wallet or two with say \$5m+ worth of BTC, and leave the rest of the wallets. Surely this would've been smarter if their end goal is spending the money... no one would've suspected a thing and blamed it on user error, considering the entropy bug has been hiding in plain sight for 5 years and no one knew about it

Weird scenario since the attacker hasn't even tried spending or laundering any of the money.

Omniscient - August 2, 2026, 9:02 pm

(Aug 2, 2026 07:07 PM)bebonzy09 Wrote: [\[CITE\]](#) You know what I've been thinking the last few days, why didn't the attacker just sweep a wallet or two with say \$5m+ worth of BTC, and leave the rest of the wallets. Surely this would've been smarter if their end goal is spending the money... no one would've suspected a thing and blamed it on user error, considering the entropy bug has been hiding in plain sight for 5 years and no one knew about it

Weird scenario since the attacker hasn't even tried spending or laundering any of the money. why commit \$5m crime when it's the same penalty and work as a \$75m crime

bebonzy09 - August 2, 2026, 9:27 pm

(Aug 2, 2026 09:02 PM)Omniscient Wrote: [\[CITE\]](#) why commit \$5m crime when it's the same penalty and work as a \$75m crime

Fair enough, but I doubt he's gonna be able to cashout that much, especially rn with his wallets publicly known and flagged.

If he ended up using this on 1-2 big coldcard victims, he could have got away imho or bought enough time to launder it out. People only started looking into it when there was mass send outs of crypto from cold card users. If it happened to a handful of people and or spread out overtime.. I think it would have been attributed to user error but that's just my opinion.

I'll be surprised if he ends up cashing this out... it seems almost impossible since he waited too long.

StuffSneak - August 3, 2026, 9:31 am

Its now over costed 1300+ Bitcoins as per last reports. I wonder what course of action they would take to cover this up.

Omniscient - August 4, 2026, 10:37 am

New development. What are the chances the dev left the entropy bug intentionally?

<https://x.com/COLDCARDwallet/status/1447213375398846473>

? loading encrypted image...

Dude in 2021 literally posted his plan. LOL

I would be so pissed if I lost BTC from this guy.

Mewtwo - August 4, 2026, 11:27 am

(Aug 4, 2026 10:37 AM)Omniscient Wrote: [\[CITE\]](#) New development. What are the chances the dev left the entropy bug intentionally?

<https://x.com/COLDCARDwallet/status/1447213375398846473>

? loading encrypted image...

Dude in 2021 literally posted his plan. LOL

I would be so pissed if I lost BTC from this guy.

I'd tell you one thing: dude had the patience to hit it all at once. In 5 years Imfao

SUI-3183372 - August 4, 2026, 5:08 pm

I tend to agree with Fatman on this one:

Kify - August 8, 2026, 3:16 am

Turns out that the author of the library containing the RNG issue, who was supposedly just a random dev whose library they liked and therefore integrated into Coldcard, used the same GPG key for multiple commits as a Coldcard developer.

The CC dev and the random dev even had public conversations with "each other". If they actually turn out to be the same person, that's pretty fishy.

Also worth noting that the supposedly random dev's Twitter account says they're from Canada, while Coinkite is a Canadian company.

<https://www.reddit.com/r/Bitcoin/s/orDNFGemYJ>

Have not checked the keys myself but this is getting blastered everywhere and no one is calling it out so I'm assuming it's correct. Note that the commits are unverified but that doesn't necessarily mean the key is spoofed.

Omniscient - August 8, 2026, 11:12 am

(Aug 8, 2026 03:16 AM)Kify Wrote: [\[CITE\]](#) Turns out that the author of the library containing the RNG issue, who was supposedly just a random dev whose library they liked and therefore integrated into Coldcard, used the same GPG key for multiple commits as a Coldcard developer.

The CC dev and the random dev even had public conversations with "each other". If they actually turn out to be the same person, that's pretty fishy.

Also worth noting that the supposedly random dev's Twitter account says they're from Canada, while Coinkite is a Canadian company.

<https://www.reddit.com/r/Bitcoin/s/orDNFGemYJ>

Have not checked the keys myself but this is getting blastered everywhere and no one is calling it out so I'm assuming it's correct. Note that the commits are unverified but that doesn't necessarily mean the key is spoofed.

Everything is a scam now. Would not put it past the NWO doing this to destroy hardware wallet confidence.

But likely just a scam for money.

Braco22 - August 8, 2026, 1:39 pm

If this ever happened while we were making new ATHs, price would collapse and it would start an avalanche, but now it just barely moved the price. Looks like the news about a hardware flaw that affected more than 1200 BTC didn't bother the retail, or simply put, the retail isn't even here.

Omniscient - August 8, 2026, 6:13 pm

(Aug 8, 2026 01:39 PM)Braco22 Wrote: [\[CITE\]](#) If this ever happened while we were making new ATHs, price would collapse and it would start an avalanche, but now it just barely moved the price. Looks like the news about a hardware flaw that affected more than 1200 BTC didn't bother the retail, or simply put, the retail isn't even here. \$100m is nothing for BTC to absorb....

Braco22 - August 8, 2026, 11:32 pm

(Aug 8, 2026 06:13 PM)Omniscient Wrote: [\[CITE\]](#) \$100m is nothing for BTC to absorb....The amount in US Dollars is not much, but the fact that something that was deemed the ultimate security (buy BTC, transfer it to a hard wallet and come back in 10 years to sell) is at the end not really secure. This combined with Ledger's Recovery thing that spiked outrage last year, and I bet that a lot of people have lost that feeling of the hardware wallets being super secure.