PRESS RELEASE

A programming flaw in Coldcard devices: $70 million in bitcoin stolen

The flaw, present for over five years, made the keys generated by Coinkite's hardware wallets vulnerable and allowed funds to be withdrawn without ever touching the devices. The attack does not appear to depend on users' operational errors. CheckSig: custody security must be verifiable by independent third parties.

Milan, August 1, 2026 - On July 30, in a 41-minute window, an attacker drained 1,196 Bitcoin addresses holding 1,082.65 BTC (approximately $70 million) protected by Coldcard hardware wallets, without resorting to phishing, malware, or physical access to the devices. A firmware flaw present since March 2021 weakened the randomness with which the devices generated the seed, the cryptographic secret from which private keys are derived, making those keys reconstructable remotely. Coinkite, the Canadian manufacturer, published a security advisory after the first reports of the withdrawals, acknowledging the flaw and distributing corrective firmware, and clarified that the update does not remedy keys already generated.

The incident

The cause is not a cryptographic attack but an implementation error: seed generation drew randomness from a software fallback function instead of the device's hardware random number generator. Sources diverge on the origin of the regression. Coinkite's advisory identifies as vulnerable the Mk3 from version 4.0.1 to 4.1.9; Block's independent analysis traces it back to version 4.0.0, released on March 17, 2021, and also includes in its scope the Mk2, which the manufacturer's advisory does not mention.

The stolen bitcoin were consolidated within minutes into four addresses. Clay Garrett, of Block, stated on July 31 that he had identified the paid account at a well-known blockchain data provider used by the attacker to query the source addresses during the withdrawals, and that the provider's internal logs match the hypothesized workflow in the number, timing, and sequence of requests; the evidence has been handed over to the authorities.

"*It will be interesting to follow on the blockchain the traces of what was stolen: laundering those bitcoin will not be easy for anyone. These are significant sums, whose origin is publicly documented and associated with a known event, on addresses the entire industry is monitoring; any attempt to put them into circulation through regulated operators will run into anti-money-laundering controls*", observes Ferdinando Ametrano, CEO of CheckSig.

Guidance for Coldcard owners

Anyone who generated their keys on vulnerable firmware must update the device, create a new seed, verify the backup and a receiving address, send a test transaction, and then transfer the remaining balance. No test exists that, by examining the seed alone, can certify

its entropy after the fact, and transferring a weak seed to another device does not fix its weakness. Ledger stated that it is not affected by the advisory, pointing to the certified random number generator embedded in its secure element; similar clarifications were issued by Trezor, Block, and other manufacturers.

The limits of self-custody

The incident reopens the debate on the limits of custody managed independently by the investor.

"*Self-custody transfers control to the investor, but along with control come technical and operational risks the investor is often in no position to observe: 'your keys, your coins' then becomes 'your keys, your problems'. The problem is not self-custody, which must always remain possible, but the idea that holding the keys automatically equals security. The affected users did nothing wrong, and our solidarity goes to them, as to all savers who are asked to assess what they lack the expertise to assess. It is reasonable to demand that this assessment be carried out by qualified, independent third parties, and that it be documented. Better, then, to rely on professional custody with no single points of failure, with documented controls, independently verified, and with contractual liability and insurance coverage: it cannot eliminate every risk, but it governs them effectively*", comments Ametrano.

Entropy must be independent of the device

Coinkite noted that users who had added at least fifty independent dice rolls during setup would have obtained robust seeds despite the flaw: randomness of external origin, combined with the device's own, would have compensated for its weakness. In distancing itself from the incident, Trezor also indicated the combination of multiple independent sources of randomness as its own safeguard.

"*The entropy used to generate a seed should not depend on the device that holds it. If the device's internal generator is the only source of randomness, it becomes a single point of failure: a flaw weakens its output without any subsequent check being able to reveal it, because a weak key is indistinguishable from a strong one until the moment someone guesses it. This is not a theoretical risk, it is what has just happened. A sound procedure combines entropy from sources independent of the device, within formalized procedures, with segregation of duties and independent controls over the related processes, as we do at CheckSig*", explains Paolo Mazzocchi, chief operating officer of CheckSig.

The CheckSig custody setup

In CheckSig's custody setup, every device is initialized with external, independent entropy: the condition that, in this incident, would have protected users who had added their own dice rolls. The infrastructure also employs devices from different manufacturers and combines manufacturers' firmware with proprietary firmware: a flaw in a single implementation cannot compromise the keys as a whole.

Moreover, in CheckSig's custody protocol, public and documented, no single key allows disposal of the funds: transaction signing requires three distinct multi-signature authorization stages, for a total of eleven keys. Unlike single signature, multi-signature eliminates the on-chain exposure of the cryptographic information an attacker would need to work back to the private keys. All the addresses hit in the incident were in fact single-signature.

In addition, the two-tier frozen/cold architecture forces an initial transfer from the frozen tier to the cold tier and imposes time locks on the cold tier that prevent the immediate transfer of funds, leaving time to detect an attempted theft and intervene.

Finally, the public proof-of-reserves demonstrates control of on-chain assets and their consistency with the declared evidence; the SOC 1 and SOC 2 Type II attestations are issued following independent audits of the controls and of their operation over the period examined; insurance coverage adds guarantees of restitution.

In any event, CheckSig does not use the affected device: none of the keys in custody was generated on a Coldcard. Even in that case, however, the safeguards described would have operated independently of the firmware flaw.

"*We do not promise the infallibility of a device, a key, or a person: we build custody in which none of these elements, on its own, is sufficient to move funds, in which the failure of any one of them can be detected, and in which controls are documented and verified by independent parties. Ours is a verifiable promise*", concludes Ametrano.

Sources

- Coinkite, security advisory on seed generation: blog.coinkite.com
- Block, *Predictable RNG fallback and 32-bit reseed in Coldcard firmware*: engineering.block.xyz
- Galaxy Research, on-chain reconstruction of the flows: x.com/glxyresearch
- Clay Garrett (Block), tracing of the operator: x.com/clay_garrett
- Ledger, statement on its devices: x.com/Ledger
- Chainalysis, on-chain analysis of July 31: x.com/chainalysis
- Trezor, statement to its users of July 31: x.com/trezor
- K33 Research, *Funds at risk: Coldcard's randomness flaw*: k33.com
- CheckSig: custody protocol, proof-of-reserves, SOC attestations

CheckSig: European Excellence as Crypto-Asset Service Provider

Founded in 2019 as a spin-off of the Digital Gold Institute — the leading European think tank on Bitcoin, crypto-assets, and blockchain — CheckSig is a Crypto Asset Service Provider (CASP) that offers advanced solutions for private and institutional investors. Its mission is to make investing in crypto-assets simple and secure, providing services for trading, custody, staking, and tax compliance. It also operates B2B and B2B2C with its Crypto-as-a-Service infrastructure CheckSig Clear (clear.checksig.com). CheckSig is:

- *the first CASP in the world to offer public proof-of-reserves since 2020;*
- *the first CASP to obtain a MiCAR in Italy;*
- *the only Italian CASP with insurance coverage — provided by a S&P AA leading insurer;*
- *the only Italian CASP with SOC 1 / SOC 2 Type II attestations — obtained through continuous audits on system and organizational controls conducted by one of the Big Four firms;*
- *since 2024, the first CASP to act as a tax withholding agent for its Italian clients.*

Press contact: press@checksig.com