COLDCARD

PUBLIC INCIDENT REPORT

COLDCARD Seed-Generation Incident

Postmortem

INCIDENT PERIOD

March 2021 – July 2026

REPORT SNAPSHOT

November 23, 2026

Current guidance and fixed-release information:
coldcard.com/security/status

Coinkite

Contents

Executive Summary

1. Factual Information

1.1 History of events

1.2 The product and its seed-generation design

1.3 libNgU

1.4 Affected and fixed releases

1.5 Losses and affected population

1.6 Pre-incident reviews

1.7 Prior concerns raised before the incident

1.8 Post-incident firmware releases

1.9 Independent verification

1.10 External events

1.11 Investigations

1.12 Customer communications and support

2. Analysis

2.1 The failure mechanism

2.2 Why the defect went undetected for more than five years

2.3 Entropy and loss estimates

2.4 How the defect was discovered: hypotheses

2.5 Adequacy of the remediation

2.6 Supply-chain integrity

3. Findings

4. Safety Recommendations

4.1 To COLDCARD users

4.2 To whoever controls the stolen funds

4.3 Closing statement

Appendix A: Keylabs Seed-Generation Review (October 15, 2026)

Appendix B: References

Executive Summary

> **COLDCARD owners:** to check whether you are affected and what to do, see Section 1.4 and Section 4.1, or the Security Status page. Never send seed words, passphrases, dice rolls, private keys, or backups to anyone.

This report was authored and published by Coinkite. It follows the structure of an NTSB accident report. Section 1 records facts and attributed statements; Section 2 contains Coinkite's analysis; Section 3 states findings; and Section 4 states recommendations. Every finding and recommendation is traceable to Sections 1 and 2.

- From March 29, 2021, through July 30, 2026, COLDCARD firmware generated wallet seeds using MicroPython's Yasmarang software pseudo-random number generator instead of the device's STM32 hardware random-number generator.
- Beginning July 29, 2026, attackers regenerated private keys for affected seeds offline and stole funds. Devices were not remotely accessed or taken over, yet some customers suffered losses. As of November 18, 2026, Coinkite has received approximately 300 loss-related support tickets associated with 242 accounts.
- Coinkite identified the defect on July 30, 2026 and published fixed firmware on July 31.
- An independent review by Keylabs, published October 15, concluded that, within its stated scope, the defect is fully closed in Mk5 5.6.3 and 5.6.2 and Q 1.5.3Q and 1.5.2Q.
- Coinkite estimates that affected seeds had roughly 40 bits (Mk2/Mk3) or 72 bits (Mk4, Mk5, Q) of effective entropy instead of the intended 128-bit security target.

Root cause: The lack of verification for which random-number implementation was actually reached by the shipping seed-generation path allowed a firmware configuration and linkage error to ship undetected.

1. Factual Information

This section records verified facts and attributed statements only.

1.1 History of events

March 1, 2021 – Coinkite integrated libNgU, changing the randomness interface used by wallet seed generation. The affected implementation is visible in the v4.0.0 source lineage.

March 29, 2021 – v4.0.1, the first signed public release in the series, shipped. v4.0.0 was not distributed as a signed public binary.

June 8, 2021 – `adlererik` publicly reviewed the Shannon-entropy calculation in COLDCARD's offline dice-roll verification tool. This work concerned adjacent tooling, not the shipping seed-generation path.

March 1–14, 2022 – `Lazy Ninja` performed a paid pre-release Mk4 security review covering PIN handling, hardware boundaries, random-number generation, and entropy hardening. The review led to changes before firmware 5.0.0 but did not identify the integration defect.

May 28, 2022 – `eugenesan` publicly reviewed the offline dice-roll tool and proposed entropy-bias calculations and other improvements. This work did not examine the shipping seed-generation path.

October 2022–May 2023 – `i5hi` independently worked through COLDCARD's reproducible-build process and contributed public verification instructions.

2023 – `Ledger Donjon` continued specialist physical-security review of complete Mk3 devices. The work concerned physical extraction rather than firmware seed generation.

September 2023 – Karim M. Abdellatif and Olivier Hériveaux of Ledger Donjon published their coordinated review of the DS28C36 used as Mk4's second Secure Element. It did not identify the firmware integration defect.

Early 2024 – Separate paid third-party review of Q.

August 7, 2024 – `mcudev` publicly reviewed user-supplied entropy and proposed a verifiable fair-coin seed-generation workflow. The proposal did not review the shipping firmware RNG path.

December 18, 2024 – `pythcoiner` and the Liana team were credited for reviewing Edge Miniscript and policy handling and reporting a policy-deserialization defect.

May 2025 – Communication between independent Bitcoin developer James O'Beirne and Coinkite concerning libNgU (see 1.7).

September 29–30, 2025 – `Nathan Landon` of Karma-X reported a Delta PIN private-key recovery issue found during a broader firmware review. Coinkite fixed it the same day.

April 9, 2026 – `Peter Severa Levashov` reported that unauthenticated USB downloads could disclose stale PSRAM data from earlier sensitive operations.

May 1–June 26, 2026 – `Rob Hamilton,` using the OpenAI Cybersecurity Harness, conducted a broad AI-assisted firmware review. It produced 85 candidate findings across security-sensitive areas and led to several fixes, but did not identify the integration defect.

May 26, 2026 – `Damir` reported a legacy-input amount and fee-display issue in the PSBT signing path.

June 2–July 3, 2026 – `dmonakhov` publicly reviewed and contributed changes concerning backup restoration, BBQr handling, and reproducible-build tooling.

June 17, 2026 – A firmware security review by `Nick Farrow,` published after the incident and dated June 17, expressly included weak RNG in its scope. It concluded that the RNG path was sound and did not identify the integration defect.

February 5, 2026 – OpenAI released GPT-5.3-Codex, the first model it classified as High capability in cybersecurity under its Preparedness Framework, and launched Trusted Access for Cyber. OpenAI said it was the first model it had directly trained to identify software vulnerabilities.

April 7, 2026 – Anthropic announced Claude Mythos Preview and Project Glasswing. Anthropic reported that the limited-release model could autonomously identify and exploit zero-day vulnerabilities.

May 7, 2026 – OpenAI introduced GPT-5.5-Cyber in limited preview to approved defenders for specialized, authorized security research, red-teaming, and penetration-testing workflows.

June 2–9, 2026 – Anthropic expanded Project Glasswing to approximately 150 organizations in more than 15 countries and introduced Mythos 5 to a small group of vetted partners.

July 16, 2026 – Kimi K3 became publicly available.

July 27, 2026 – Kimi K3 full model weights were released.

July 29, 2026 – Unexpected transactions involving affected seeds began, per independent reporting.

July 30, 2026 – Users discovered thefts. Public reports alerted Coinkite. Coinkite began incident response, identified the defect, and published an initial security advisory. Unshipped COLDCARD stock was quarantined at the factory, and later decommissioned.

July 31, 2026 – Fixed firmware was published for supported standard, legacy, and Edge tracks.

August 1, 2026 – `Christopher David` of OpenAgents ran the Loupe audit workflow against the pre-fix firmware. Its default checkout omitted dependency submodules and missed the defect; the same workflow found it after the submodules were populated.

August 2, 2026 – `Medusa` reported that Claude Code found the already-public defect in eight minutes and later reported a GLM 5.2 hit without web access. These were post-disclosure reproductions, not blind discovery.

August 3, 2026 – Fixed firmware was deployed to the factory and COLDCARD hardware production restarted.

August 3–4, 2026 – `Lloyd Fournier` reused Nick Farrow's audit prompt across several models. He reported misses for Claude Opus 5 xhigh, GLM 5.2, Qwen3-Coder-Next, and Gemini 3.6 Flash high, and hits for GPT-5.6 Sol max and Kimi K3.

August 4, 2026 – `TheIcarusWings` published a Claude Fable 5 transcript that found and explained the defect after first reading the public fix diff. This was source-grounded validation, not blind discovery.

August 5, 2026 – Bitcoin Red Team began a human-guided, multi-model review of Bitcoin software.

> **August 14, 2026 –** Galaxy Research reported 1,778.84 BTC stolen from more than 8,600 addresses, based partly on direct contact with 190 people reporting alleged losses.

> **August 20, 2026 –** Mk4/Mk5 5.6.1 and Q 1.5.1Q were published.

> **August 31, 2026 –** Edge 6.6.1X and 6.6.1QX were published.

> **September 3, 2026 –** Mk4/Mk5 5.6.2 and Q 1.5.2Q were published.

> **September 30, 2026 –** Mk4/Mk5 5.6.3 and Q 1.5.3Q were published.

> **October 8, 2026 –** Coinkite completed its support review (see 1.5).

> **October 13, 2026 –** Ledger reported an unrelated hardware-implant incident (see 1.10).

> **October 15, 2026 –** Keylabs published its independent seed-generation review.

1.2 The product and its seed-generation design

COLDCARD is a non-custodial, Bitcoin-only hardware wallet. Its seed generation was intended to draw exclusively from the STM32 hardware RNG; the firmware was not designed to fall back to a software generator.

In affected builds, libNgU's rng_get() symbol resolved to MicroPython's Yasmarang general-purpose pseudo-random number generator instead of the board-specific STM32 hardware generator. Keylabs traced the path as follows:

1. COLDCARD's firmware configuration set MICROPY_HW_ENABLE_RNG to zero.
2. An ineffective guard in the pinned libNgU code accepted that configuration.
3. rng_get() resolved to MicroPython's software generator.

The hardware generator did not fail at runtime and no fallback was triggered. Both implementations exposed a compatible interface.

The firmware built, and seed creation appeared to work, and the device produced well-formed seed words. The intended hardware (TRNG) implementation was present in the firmware but was not reached by seed generation. Seed output was hashed before use.

The incorrect backend selection was triggered by COLDCARD's firmware configuration. It was a COLDCARD integration defect, not a defect in libNgU itself. Keylabs also identified an ineffective configuration guard in the pinned libNgU code as a contributing control failure.

Not involved: COLDCARD's physical-security layers, libsecp256k1, duress features, and transaction authorization controls. Attackers did not need physical access to or control of a device.

1.3 libNgU

In March 2021, Coinkite changed COLDCARD's embedded cryptographic stack to use Bitcoin Core's libsecp256k1 through an embedded wrapper called libNgU. Coinkite CTO, Peter Gray, writing under the pseudonym `Switck,` developed libNgU as a standalone project rather than a COLDCARD-specific component. Pseudonymous participation is common in Bitcoin development, which began with a pseudonymous author.

libNgU's purpose was to make libsecp256k1 practical on embedded MicroPython platforms and reusable by other commercial Bitcoin projects. At the time, Coinkite was not aware of any other maintained integration for that environment. Its source was public and commercially reusable by qualifying Bitcoin projects under its own Bitcoin-only license.

Adopting libNgU removed COLDCARD's remaining GPL dependency. The rest of the firmware was then distributed under MIT plus the Commons Clause, which remained commercially restrictive; libNgU could be reused commercially by qualifying Bitcoin projects under its own license.

1.4 Affected and fixed releases

Model and release track	Seed generated on affected firmware	Minimum fixed release
Mk2/Mk3	4.0.1 through 4.1.9	4.2.0 or later
Mk4/Mk5 standard	Before 5.6.0	5.6.0 or later
Mk4/Mk5 Edge	Before 6.6.0X	6.6.0X or later
Q standard	Before 1.5.0Q	1.5.0Q or later
Q Edge	Before 6.6.0QX	6.6.0QX or later

Current standard releases: 5.6.3 (Mk4/Mk5) and 1.5.3Q (Q). Current Edge releases: 6.6.2X (Mk4/Mk5) and 6.6.2QX (Q). Standard and Edge are separate tracks with independent version numbering.

Scope rules: a seed securely generated outside the affected on-device flow was not weakened by later import into an affected device. A seed generated on affected firmware remains affected after being restored, imported, backed up, or cloned.

Seeds generated with at least 50 fair, independent, private dice rolls entered through Add Dice Rolls, with the sequence never recorded or exposed and the final post-roll words used, were not weakened by the defect.

1.5 Losses and affected population

Measure	Count	Source and date
Distinct seed roots reconstructed from the first theft wave	at least 328	Public Wave 1 analysis
Loss-related support tickets	300	Coinkite support review, November 18, 2026
Requester accounts behind those tickets	242	Coinkite support review, November 18, 2026
Attributed addresses	8,865	Galaxy Research, as of August 24, 2026

As of November 18, Coinkite's support review identified 300 loss-related tickets associated with 242 requester accounts. Those accounts correspond to approximately 0.21% of the estimated COLDCARD user base. Separately, one public Wave 1 analysis reported reconstructing 328 seed roots, and Galaxy Research reported more than 8,600 addresses. These measures count different populations: seeds, tickets, requester accounts, and addresses.

One seed can derive many addresses; one person can control multiple seeds; reports can duplicate the same loss or remain unverified; and some victims may have lost more than one seed. Duplicate review remained open as of November 18. No public total of affected users or losses across every theft wave has been established.

1.6 Pre-incident reviews

Between 2021 and 2026, we documented at least 15 independent review and security-research efforts on COLDCARD hardware, firmware, entropy tooling, and release controls, including two commissioned third-party product reviews, including the following:

- `Lazy Ninja` issues a paid, pre-release Mk4 review covering PIN handling, hardware boundaries, random-number generation, and entropy hardening in March 2022.
- A separate, paid, third-party review of Q took place in early 2024. The reviewer's name and exact artifact scope are not included in the current public record.
- Ledger Donjon researchers `Olivier Hériveaux` and `Karim M. Abdellatif` examined physical attacks against Mk3 and Mk4 hardware during the affected period.
- `pythcoiner` and the Liana team, `Nathan Landon` of Karma-X, `Peter Severa Levashov,` `Damir,` and `dmonakhov` reviewed and reported issues in other firmware surfaces.
- Public contributors `adlererik`, `eugenesan`, `i5hi`, and `mcudev` examined adjacent entropy or reproducible-build tooling. These were contributions and targeted reviews, not full firmware audits. Our source code was public throughout, with 54 contributors to the firmware repository.
- `Rob Hamilton` used the OpenAI Cybersecurity Harness for a broad AI-assisted review from May 1 through June 26, 2026. It generated 85 candidate findings and led to several fixes.
- A review by `Nick Farrow` dated June 17, 2026 expressly included weak RNG, concluded the RNG path was sound, and did not identify the defect.
- Coinkite maintainers, including `doc-hex` and `scgbckbone`, reviewed and tested releases throughout the affected period.

The scope for each of these review processes varied substantially. Not all of this work examined seed generation, and not all of it was a full product or release review. No contemporaneous report from these reviews identified and reproduced the specific build-integration defect that caused `rng_get()` in the shipping seed-generation path to resolve to MicroPython's Yasmarang generator.

Before the incident, releases used signed manifests, public source, reproducible-build tooling, functional tests, and statistical RNG-output tests. Those controls verified provenance, build repeatability, basic behavior, and output characteristics. They did not verify which RNG implementation the shipping seed-generation path actually reached. That missing path check is why the defect survived otherwise useful controls.

1.7 Prior concerns raised before the incident

In May 2025, independent Bitcoin developer James O'Beirne raised a concern about libNgU's quality and recommended removing libNgU. O'Beirne did not identify or document a specific defect, and he did not pursue the report further. (Note: The defect was in COLDCARD's integration of libNgU, not in libNgU itself.)

1.8 Post-incident firmware releases

July 31, 2026 (fixed releases, all supported tracks).

- Corrected the seed-generation path.
- Added a build-time check that rejects a build if libNgU's random-byte path resolves to the wrong implementation.
- Affected historical releases were marked in the download archive and model-specific migration guidance was published.

August 20, 2026 (Mk4/Mk5 5.6.1 and Q 1.5.1Q).

- Every newly generated master seed, generated Temporary Seed, and generated CCC Key C requires one user-input method: at least 65 physical key presses with unpredictable timing, 50 physical six-sided-die rolls, or 128 physical coin flips.
- The standard flow combines that input with output from the STM32 hardware RNG, fresh entropy from Secure Element 1, and from Secure Element 2.
- libNgU's general-purpose generator is upgraded to SHA-256 Hash_DRBG instead of Yasmarang.
- Firmware checks hardware-RNG error states, retries bounded recoverable faults, and stops on a persistent fault.
- At boot, firmware checks that rng_get() in the running build enters the intended hardware-read path; if not, the device stops before normal operation.
- Dice Rolls Only remains a separate advanced workflow that excludes hardware entropy and requires 50 rolls (12-word seed) or 99 rolls (24-word seed).
- Additional fixes from a broader review: rechecking a staged PSBT immediately before signing; blocking SIGHASH_SINGLE by default; restricting USB downloads to the current encrypted-session result; rejecting firmware data beyond the signed length; strengthening Delta Mode isolation; making active-wallet display and backup behavior more explicit.

The broader review covered surrounding seed-generation paths, transaction signing, USB data handling, firmware-update validation, Delta Mode, and backups. The firmware changelog lists the complete changes, model scope, credits, and compatibility. The SeedFlow map traces current seed generation on Mk4/Mk5 5.6.1+ and Q 1.5.1Q+.

August 31, 2026 (Edge 6.6.1X and 6.6.1QX). Signed Edge releases. Edge is a separate preview track for developers and early adopters.

September 3, 2026 (Mk4/Mk5 5.6.2 and Q 1.5.2Q). Restored View TRNG Words, which displays the complete 256-bit device-generated input before user entropy is mixed in. Added the public-domain, dependency-free verify_seed_mix.py tool for recomputing a final seed from the displayed TRNG words and a complete dice-roll or coin-flip sequence.

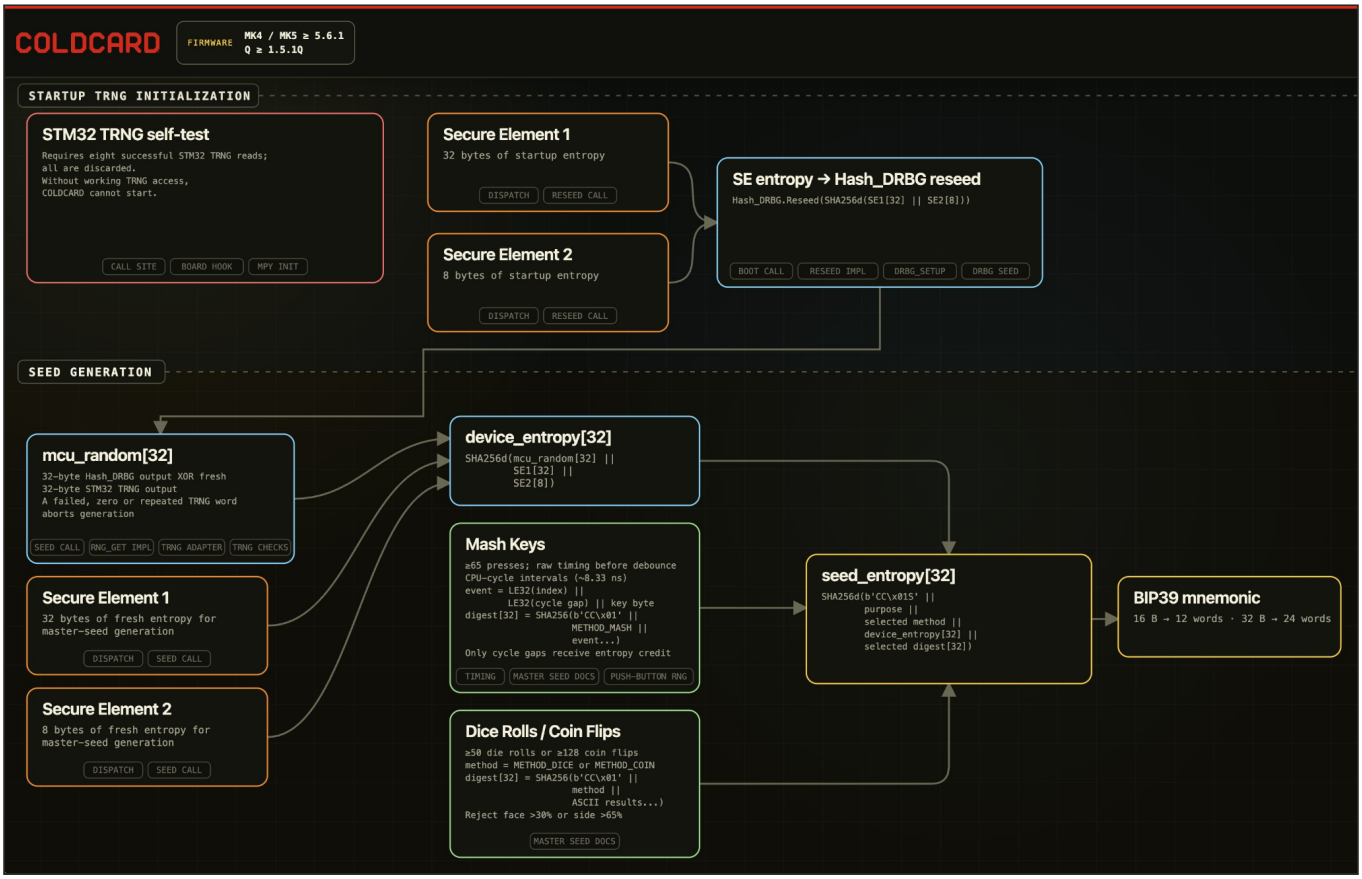
September 30, 2026 (Mk4/Mk5 5.6.3 and Q 1.5.3Q). Added Codex32 wallet generation and recovery, Shamir backups, optional Seed Vault names, stricter PSBTv2 parsing and locktime checks, firmware signer and downgrade warnings, and additional signing and QR-scanning safeguards. Retains the corrected RNG path, required user entropy, View TRNG Words, and seed-mixing verification.

1.9 Independent verification

Independent researchers performed the following scoped checks: real-device instrumentation of the Mk4 5.6.0 hardware-RNG path; source review across the fixed release lines; review of the hotfix mechanics; and a reproducible build and dice-path trace for Mk4/Mk5 5.6.0.

Keylabs published *COLDCARD Seed Generation Review*, version 1.0, on October 15, 2026. Within its stated scope, Keylabs found the remediation sound, confirmed it in the shipped binaries, identified no remaining item required to close this vulnerability class, and concluded the July 2026 build integration defect is fully closed.

Artifacts, methods, and limitations are detailed in Appendix A. The public report is available at https://blog.coinkite.com/reports/coldcard-seed-generation-review-keylabs-2026-10-15.pdf and from the Security Status page.



Explore the interactive, source-linked SeedFlow map to trace current seed generation on Mk4/Mk5 5.6.1 or later and Q 1.5.1Q or later.

1.10 External events

Kimi K3. Became publicly available July 16, 2026; full model weights released July 27, 2026. Third-party variants with deliberately reduced refusal behavior have since circulated.

Bitcoin Red Team. In the days following public disclosure of the COLDCARD integration defect, Bitcoin Red Team organized a human-guided, multi-model review of Bitcoin software using Kimi K3 extensively. After 108 hours, organizers reported 7,958 candidate findings across 501 projects, with 24.7% then having reproducible proofs of concept, and reported that Kimi accounted for 74% of their model spending. Some resulting issues were subsequently validated or patched. The campaign began after the COLDCARD integration defect was public.

Disclosure volume. Coinkite and other hardware and software projects across the Bitcoin ecosystem are receiving an exceptionally high volume of candidate security findings and disclosures. The tools that produced individual reports cannot be verified.

Ledger hardware implant. On October 13, 2026, Ledger reported that an unauthorized hardware implant in an affected device sold through authorized reseller CryptoBilis read recovery words from the display path and transmitted them over LTE, leaving the Secure Element and operating system unchanged. That incident is under investigation and is technically unrelated to the COLDCARD integration defect.

1.11 Investigations

Law enforcement is actively investigating the thefts and those responsible. The Canadian Centre for Cyber Security has a separate open case concerning the incident. Investigation, attribution, and enforcement are the responsibility of law enforcement. Who carried out the thefts and how the defect was discovered are unknown.

Blockchain analysis firms are watching the transactions of the attackers and will report to the public if and when funds are moved.

1.12 Customer communications and support

- Coinkite has published an advisory, technical backgrounder, migration guide, download-archive markings, and a Security Status page.
- Support is recording reports, helping customers verify firmware, and guiding migration. The team is stretched across disclosure triage, incident response, and support; response times are longer than usual.
- Coinkite previously honored requests to blank customer email addresses where possible and has added category-level notification preferences. Addresses previously blanked cannot be restored, but customers may re-subscribe to individual topics, if they wish.
- Coinkite is evaluating all possible options to support customers who suffered losses. Any program will be announced only once its scope and terms are settled. We will share details when they are available.
- Coinkite has received reports that some influencers and educators charged customers for wallet mentoring and advised placing substantial savings in single-signature wallets without a strong BIP-39 passphrase, private dice rolls, or multisig.
- Coinkite has publicly asked whoever controls the stolen funds to return them via security@coinkite.com, without promising immunity, confidentiality, payment, or any particular outcome.

2. Analysis

This section contains Coinkite's interpretation of the facts in Section 1. Where an inference is uncertain or disputed, it says so.

2.1 The failure mechanism

The defect was a silent substitution, not a runtime failure. Because Yasmarang and the STM32 driver exposed compatible interfaces, the build system had no reason to reject the link, and the device had no error to report. The safeguard that should have caught the configuration, the libNgU guard against MICROPY_HW_ENABLE_RNG being zero, did not work.

Hashing the generator's output changed its form but could not add entropy that was not there. A seed with roughly 40 or 72 bits of entropy is within reach of offline brute-force regeneration, which is consistent with attackers needing no device access.

2.2 Why the defect went undetected for more than five years

Every check Coinkite ran answered a nearby question rather than the critical one. Release checks confirmed the hardware-RNG code was present (1.6), not that seed generation reached it. Functional tests confirmed seed words were well formed, which they were.

The statistical output-health tests examined by Keylabs could not distinguish the defective generator from a properly seeded one. A finite sample of output cannot establish which entropy source produced it; the missing check was verification of the resolved seed-generation path in the shipping firmware (Appendix A).

External reviews (1.6) varied in scope and were not tied to verifying this specific path in specific release artifacts. Public source and reproducible builds made the defect inspectable but did not cause anyone to inspect this path.

2.3 Entropy and loss estimates

The ~40-bit (Mk2/Mk3) and ~72-bit (Mk4/Mk5/Q) figures are Coinkite's internal estimates.

The loss figures in 1.5 measure different populations and cannot be combined into a victim count. The true affected population is likely larger than 242 accounts, since not every victim files a ticket, but no confirmed total exists. Because COLDCARD is noncustodial, Coinkite cannot produce a complete count from its own data. The range may change as seed reconstruction, claimant deduplication, and transaction attribution continue.

2.4 How the defect was discovered: hypotheses

This is unresolved and is not an attribution. The interval between Kimi K3's full weight release (July 27) and the first thefts (July 29) is short enough that AI-assisted discovery is a plausible hypothesis.

The Bitcoin Red Team campaign (1.10) began after disclosure, so it is evidence of the model's contemporaneous capability and adoption for exactly this kind of security research, not evidence of who found this defect.

Wider access to capable models, including reduced-refusal variants, is plausibly contributing to the current volume of disclosures, but the tools behind individual reports cannot be verified at this time.

2.5 Adequacy of the remediation

The July 31 fix corrected the path and added a build-time gate. Later releases added required user entropy, STM32 TRNG output, fresh entropy from Secure Element 1, Secure Element 2's static per-device value, boot-time path verification, and fail-closed RNG handling. A repeat of the same linkage error would now be caught at build time, caught at boot, or mitigated by user-supplied entropy.

These controls verify specific paths and failure states. They do not prove arbitrary randomness and are not a claim that the firmware is free of every possible defect. Keylabs' review supports the remediation for the four named standard binaries; Edge releases and other components were outside its scope. No firmware change repairs seeds already generated on affected firmware.

Current review work is tied to pinned source revisions and release artifacts. Candidate findings are reproduced and tested against complete call paths; rejected findings record the guard that defeats them; fixes receive focused regression tests; and the final release delta is rechecked after fixes merge. Keylabs separately verified the repaired seed path in source and four signed standard-release binaries using a pre-fix binary as a negative control.

2.6 Supply-chain integrity

The Ledger incident (1.10) is a different failure mode but reinforces a shared lesson: no authenticity check, secure element, firmware signature, or tamper-evident package can by itself prove the integrity of an entire device and distribution chain.

Layered checks may reveal substitution or tampering but are not a guarantee against every hardware implant. Visual inspection can complement provenance checks, but it cannot establish the absence of concealed or substituted hardware.

3. Findings

1. Across the affected Mk2/Mk3, Mk4/Mk5, and Q releases, COLDCARD seed generation used MicroPython's Yasmarang software generator instead of the STM32 hardware RNG until the July 31, 2026 fixes. (1.1, 1.2, 1.4)
2. The cause was a firmware configuration (MICROPY_HW_ENABLE_RNG set to zero) that an ineffective guard in the pinned libNgU code accepted, resolving rng_get() to the software generator. (1.2)
3. The defect was not in libsecp256k1, and not in COLDCARD's physical-security, duress, or transaction-authorization controls. (1.2)
4. Affected seeds had approximately 40 bits (Mk2/Mk3) or 72 bits (Mk4/Mk5/Q) of effective entropy by Coinkite's estimate, against a 128-bit security target. The 72-bit figure has not been independently established. (2.3)
5. Attackers stole funds by regenerating affected private keys offline, beginning July 29, 2026. No device access was required. (1.1, 1.2)
6. Coinkite's release checks verified the presence of the hardware-RNG code but not which implementation the shipping seed-generation path reached. This was the missing release gate. (1.6, 2.2)
7. The statistical output-health tests examined could not have detected the defect; the defective generator could pass those tests. Verification of entropy provenance and the resolved seed-generation path was required to identify the defect. (1.6, 2.2)
8. Paid third-party reviews in 2022 and 2024, public scrutiny, and AI-assisted reviews did not identify the defect; none was tied to verifying this path in specific release artifacts. (1.6, 2.2)
9. In May 2025, a reviewer raised general quality concerns, and recommended removing libNgU. The specific integration defect related to RNG was not identified. (1.7)
10. Coinkite identified the defect on the day of public reports (July 30) and published fixed firmware for all supported tracks the following day. (1.1, 1.8)
11. Subsequent releases added required user entropy, multiple hardware entropy sources, build-time and boot-time path verification, and fail-closed RNG handling. (1.8, 2.5)
12. Keylabs confirmed, within its scope, that the defect is fully closed in Mk5 5.6.3/5.6.2 and Q 1.5.3Q/1.5.2Q. Edge releases were not reviewed. (1.9, Appendix A)
13. Firmware updates do not repair seeds generated on affected firmware; affected users must migrate to a new seed. (1.4, 2.5)
14. The number of affected customers and total losses are not known. One public Wave 1 analysis reported 328 reconstructed seed roots; Coinkite's support review identified 242 requester accounts; and Galaxy Research publicly reported more than 8,600 addresses. These measures count different populations. (1.5, 2.3)
15. Who discovered and exploited the defect is unknown. AI-assisted discovery is a plausible hypothesis, not an attribution. (1.10, 1.11, 2.4)

4. Safety Recommendations

Twelve recommendations to Coinkite are implemented and three remain open. Status is tracked on the Security Status page.

No.	Recommendation	Status
C-1	Verify the resolved seed-generation path at build time and again in running firmware at boot.	Implemented (July 31 build gate; 5.6.1/1.5.1Q boot check)
C-2	Fail closed on persistent hardware-RNG faults.	Implemented (5.6.1/1.5.1Q)
C-3	Require user-supplied entropy and combine it with independent hardware sources for every generated seed.	Implemented (5.6.1/1.5.1Q)
C-4	Remove the weak software generator from libNgU's general-purpose path.	Implemented (SHA-256 Hash_DRBG, 5.6.1/1.5.1Q)
C-5	Give users a way to verify seed mixing independently.	Implemented (View TRNG Words and verify_seed_mix.py, 5.6.2/1.5.2Q)
C-6	Tie security claims to signed releases and state the scope of the supporting check.	Implemented
C-7	Tie paid third-party reviews to specific release artifacts and require them to state which security-critical paths were and were not tested.	Implemented
C-8	Publish direct private-reporting instructions in the firmware repository.	Implemented
C-9	Make internal pull requests and code discussions more available for public scrutiny.	Implemented
C-10	Maintain one dated public record for release guidance, migration, verification evidence, and corrections.	Implemented (Security Status page)
C-11	Publish the Keylabs report PDF here and on the Security Status page.	Implemented (Appendix A; Security Status page)
C-12	Commission further independent reviews tied to specific release artifacts, including Edge, and publish scope, findings, remediation, and retest status.	Open
C-13	Ship category-level email notification preferences.	Implemented
C-14	Restore and confirm control of the @COLDCARDwallet X account.	Open
C-15	Decide on and publish any compensation or assistance plan for affected customers.	Open; no decision

4.1 To COLDCARD users

No.	Recommendation
U-1	If your seed was generated on affected firmware, install verified fixed firmware, create a new seed, verify it and its backup, and move your funds. Migrate passphrase wallets too.
U-2	Never send seed words, passphrases, dice rolls, private keys, backup files, or backup passwords to anyone, including Coinkite, or enter them into any website.
U-3	Use only support routes linked from coldcard.com. Treat unsolicited recovery, migration, or compensation offers as likely impersonation.
U-4	For material amounts, add independent layers: genuine private dice rolls; a strong, unique, separately backed-up BIP-39 passphrase with recorded fingerprint and tested recovery; multisig where its complexity fits your threat model. These do not repair an affected seed.
U-5	Inspect the numbered tamper-evident bag and clear case, verify the bag number on first boot, and install current verified firmware before creating or importing a seed.
U-6	Keep security and firmware notifications enabled. If you previously asked to have your email blanked, resubscribe.
U-7	If you paid for advice connected to an affected wallet, preserve invoices, messages, course materials, and setup instructions.

4.2 To whoever controls the stolen funds

Return them. Some victims lost life-changing amounts, and returning the funds is the only action that can directly reduce that harm.

Contact security@coinkite.com to establish a verified channel and work through counsel on a lawful return process. Do not contact victims directly or request wallet secrets.

Coinkite cannot promise immunity, confidentiality, payment, or any particular outcome, but will engage in good faith.

4.3 Closing statement

Trust is not rebuilt by saying that a release is secure or that a process has improved. It is rebuilt release by release: by acknowledging failures, making customer action unambiguous, publishing inspectable fixes, crediting valid reports, and stating what the evidence does and does not prove. That is the standard Coinkite expects users and researchers to hold it to.

No firmware release or report can undo the losses customers suffered. Coinkite is grateful to its team, dozens of independent researchers, competitors, the Bitcoin Red Team, and everyone across the Bitcoin security community who reported issues, reproduced edge cases, reviewed fixes, or helped users migrate. Their work has made the current releases stronger.

Verified updates will continue as investigation and remediation proceed.

Appendix A: Keylabs Seed-Generation Review (October 15, 2026)

Item	Detail
Reviewed artifacts	Mk5 5.6.3 (7b4d6cc4) and 5.6.2; Q 1.5.3Q (282b8a4f) and 1.5.2Q; release tags 2026-09-30T2026-v5.6.3 and 2026-09-03T1541-v5.6.2; pinned libNgU 4d9af84 and MicroPython 3d227fe; four shipped DFU images; Mk5 5.5.1 as pre-fix negative control.
Methods	Source and pinned-submodule review; signed-release hash verification; GNU objdump disassembly of four current images and one pre-fix image; simulation of the original defective generator.
Firmware integrity	Each image's SHA-256 checked against PGP-signed signatures.txt. Current images reach the STM32 RNG data register. The pre-fix image contains Yasmarang and does not reach the hardware peripheral in that path.
Controls verified	(1) value-checked compile-time guard; (2) build-time removal and symbol poisoning of the software fallback; (3) build-time relocation-chain check proving rng_get() terminates at the board hardware driver; (4) boot-time self-test reaching the hardware path before normal operation. Full 256-bit Secure Element boot reseed confirmed.
Simulation	The old generator could pass the statistical health tests examined.
Release-pair consistency	RNG-path C code byte-identical within 5.6.2/5.6.3 and 1.5.2Q/1.5.3Q.
Conclusion	Remediation sound and confirmed in shipped binaries; no remaining item required to close this vulnerability class; July 2026 defect fully closed.
Limitations	Limited to the seed-generation fix in the four named standard binaries. Not a full audit of every model, release track, feature, component, or runtime state. Edge releases not covered. ~72-bit estimate not independently established. Does not repair affected seeds or change migration guidance.

Appendix B: References

CUSTOMER RESOURCES

- Current Security Status
- Affected-Seed Migration Guide
- Firmware Downloads and Historical Archive
- Verify and Install Firmware
- Quick Start: tamper-evident bag and case inspection
- Codex32 Guide

COINKITE ADVISORIES AND RELEASE NOTES

- Original Security Advisory
- Technical Backgrounder
- Adding to the Public Record
- August 20 Firmware Security Update
- September 3 Firmware Security Update
- September 30 Firmware Update
- Firmware Changelog

SOURCE AND TECHNICAL

- Initial libNgU integration commit
- libNgU
- SeedFlow map

INDEPENDENT REVIEW

- Keylabs, *COLDCARD Seed Generation Review*, **version 1.0 (October 15, 2026; https://blog.coinkite.com/reports/coldcard-seed-generation-review-keylabs-2026-10-15.pdf)**
- Keylabs

EXTERNAL CONTEXT

- Kimi K3 release
- **Bitcoin Red Team:** findings, proofs of concept, model spend
- Ledger implant report
- Canadian Centre for Cyber Security

Contact: security@coinkite.com