Funds at risk, Coldcards randomness flaw

Coldcard wallets generated with insufficient randomness led to funds being stolen. Elsewhere, the Federal Reserve held interest rates steady, New York sued Kalshi over alleged illegal gambling operations, and Coinbase reported second quarter earnings.

This Week's Main News

Coinbase slips despite solid results

Coinbase shares fell about 7% in after-hours trading after the company reported second-quarter results, even as it highlighted strong momentum across its expanding business lines. Prediction market contracts and revenue more than doubled from the previous quarter, surpassing $100 million in annualized revenue, while Coinbase captured a record 10.3% share of global crypto trading volume for its third straight quarter of market share gains.

The exchange said its diversification strategy continues to reduce reliance on bitcoin spot trading. Average USDC holdings on the platform reached a record $20 billion, subscription and services revenue rose to $555 million, and 88% of net revenue now comes from sources other than bitcoin spot trading. Coinbase also reported its 14th consecutive quarter of positive adjusted EBITDA, supported in part by AI-driven productivity gains.

Fed keeps rates unchanged

The Federal Reserve kept its benchmark interest rate unchanged at 3.5% to 3.75% in a 9-3 vote, with three policymakers dissenting in favor of a quarter-point rate hike. The Fed cited solid economic growth but said inflation remains above its 2% target due in part to higher energy prices and supply shocks, while officials signaled they will remain cautious as geopolitical risks add uncertainty to the outlook.

New York sues Kalshi

New York has sued prediction market platform Kalshi, alleging it operates an illegal gambling business by offering unlicensed sports, culture and election betting. The state is seeking to block Kalshi's operations, require restitution to users, recover alleged profits and impose penalties that could total at least $36 billion following a full accounting.

The lawsuit adds to mounting legal pressure on Kalshi, which is facing enforcement actions in several states over its event contracts. The case also highlights an ongoing jurisdictional dispute between state regulators and the Commodity Futures Trading Commission, which argues it has primary oversight of federally regulated prediction markets.

NFL seeks tighter prediction market rules

The NFL has urged the Commodity Futures Trading Commission to strengthen its proposed rules for sports prediction markets, arguing they do not go far enough to protect game integrity and consumers. The league called for tighter restrictions on easily manipulated markets, stronger insider trading rules, longer review periods for new contracts, and safeguards including a minimum betting age of 21, advertising limits and a ban on margin trading.

In a sentence

- Strategy extends bitcoin pause to five weeks, sells $544.5 million in MSTR as USD reserve hits $3.75 billion
- Russia's central bank drafts first rules for 'organized' crypto trading
- Russia detains crypto mining firm BitRiver founder on fraud charges: report

Trending Topics

Coldcard randomness flaw puts Bitcoin at risk

A serious firmware flaw has put bitcoin wallets created on several Coldcard models at risk. The problem concerns the randomness used when generating a wallet seed, which is the secret foundation of the wallet.

In simple terms, some Coldcards created secrets that were easier to guess than they should have been. An attacker who reproduces an affected seed can steal the bitcoin without touching the device.

A hardware wallet must use highly unpredictable data when creating a seed. On affected Coldcards, the software sometimes bypassed the intended hardware random-number generator and used a predictable software fallback instead. The resulting seed could look random while containing far less real randomness than required.

The flaw entered Coldcard's code during a major rewrite in March 2021. Coinkite was moving elliptic-curve operations to Bitcoin Core's libsecp256k1 through the libNgU library.

The library itself was not the issue. The problem was its integration. Seed generation was moved from Coldcard's own randomness function to a path that unexpectedly connected to MicroPython's Yasmarang software generator rather than the device's hardware source.

On affected Mk2 and Mk3 firmware, this fallback was seeded mainly with part of the device identifier, a timer, and the history of software calls. These values provide limited secrecy. Under the right conditions, an attacker could search through the possible seeds and identify the corresponding wallet.

Mk1 is reported as unaffected. Older Mk2 and Mk3 firmware, before the 4.x series, used the hardware generator directly and are also reported as unaffected. Mk2 and Mk3 devices running affected 4.x firmware face the greatest exposure. The supplied advisories differ slightly on whether the vulnerable range begins with version 4.0.0 or 4.0.1.

Mk4, Q, and Mk5 are also affected on firmware released before the fixes. These models added randomness from secure elements during startup, making an attack harder, but the implementation retained too little of that input. Block says the reseed contributed only 32 bits of secret entropy. Coinkite gives a preliminary estimate of about 72 bits of effective security under its assumptions. Both agree that the protection fell below the intended standard.

The issue was discovered on July 30, 2026, after Block's Bitcoin engineering and security teams investigated reports of non-Bitkey wallets being remotely drained. Researchers traced the problem to Coldcard's random-number path, disclosed their findings to Coinkite, and published a technical analysis. Coinkite acknowledged that it had not previously known about the flaw.

Updating the firmware does not repair a seed created by affected software. The user must generate a completely new seed on fixed or unaffected hardware and move the funds to addresses derived from it.

A seed exported from an affected Coldcard remains vulnerable in another wallet. A strong passphrase or at least 50 fair, private dice rolls used during the original setup may provide additional protection. Users should verify the new wallet, send a small test transaction, and then move the remaining funds.

Recommended Reading

From our analysts

- **Slowest month since 2023:** Bitcoin is having its quietest month since 2023, falling 3% over the past week as BTC remains stuck around $60-66k. Slowing activity is crushing revenues, leading to exchange closures, with legendary pioneer BitMEX announcing its shutdown this week.

Reading

- **More than a year ago, the House passed the Clarity Act:** Scott Bessent urges the Senate to vote on the Clarity Act.