— BRIEFING / 022 · SEPTEMBER 2026

COLD STORAGE IS A SUPPLY CHAIN

The largest hardware wallet exploit on record did not touch a single device. It exploited a decision made in a build configuration five years ago, and it teaches the discipline every serious holder now owes their own custody stack.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

— 01 / WHAT HAPPENED

WHAT HAPPENED

Beginning July 30, an attacker or attackers systematically swept bitcoin from wallets whose seeds had been generated on Coldcard hardware devices. The first wave emptied roughly 1,200 addresses of about 1,083 BTC in 41 minutes. Three further waves through August 3 brought the total to approximately 1,800 BTC across more than 5,000 addresses, between $114 and $116 million at prevailing prices. The vendor, Coinkite, shipped emergency firmware within a day, halted shipments, and destroyed affected inventory. Blockchain intelligence tracking shows most stolen funds pooling at a small number of attacker addresses with minimal laundering so far, and analysts caution the full victim count will take months to emerge.

$116M DRAINED JULY 30 TO AUGUST 3

41 MIN FOR THE FIRST SWEEP OF ~1,200 ADDRESSES

5 YRS THE FLAW SAT IN THE FIELD BEFORE WEAPONIZATION

— 02 / THE ROOT CAUSE

THE ROOT CAUSE

The flaw traces to a firmware release from March 2021. A build configuration error caused seed generation on affected devices to fall back from the hardware entropy source to a weak software random number generator, collapsing effective key strength far below design. Keys that owners reasonably believed were unguessable became, for a subset of devices, reconstructable offline by an attacker with modern computing power and public blockchain data. Researchers had flagged the weakness in 2025. This summer, someone finished the work. Critically, the patch does not repair existing seeds: any seed generated on an affected device in the window must be treated as compromised and migrated.

— 03 / THE STRUCTURAL LESSON

THE STRUCTURAL LESSON

The instinctive reading, that one vendor failed, misses the point ERS would put in front of every fund and family office. Cold storage is not a product. It is a supply chain: silicon, entropy sources, firmware, build configuration, release processes, and the human review wrapped around each. Assurance at one layer does not transfer to the others, and marketing language transfers to none of them. A five-year gap between introduction and weaponization also means the relevant question is never whether your device is currently being exploited. It is whether you would know which of your keys were exposed if an advisory landed tomorrow morning.

— 04 / THE DISCIPLINE

THE DISCIPLINE

Three practices convert this incident into preparation. First, inventory: know which devices, firmware generations, and generation dates stand behind every key you or your organization controls, including keys held by founders personally. In this incident, exposure was defined by a date range and a firmware lineage; holders without records could not even assess themselves. Second, advisory response: treat vendor security advisories as operational events with an owner and a clock, because this attacker moved in minutes and the gap between disclosure and sweep is the whole game. Third, rehearsed migration: moving significant value under time pressure involves fee decisions, signing logistics, and destination verification that go badly when improvised. The holders who fared best this summer had practiced.

— 05 / THE WIDER READ

THE WIDER READ

Self-custody remains a sound principle for those equipped to operate it, and this incident does not reverse that. What it ends is the era of assumed assurance. Verification per device generation, documented inventory, and rehearsed response are now the price of the confidence that hardware wallets used to sell on the box.

— 06 / SOURCES AND METHOD

SOURCES AND METHOD

This briefing draws on TRM Labs analysis, Bloomberg, CBC, and technical reporting from July 30 to mid-August 2026. We describe the vulnerability at class level only and identify no victims. The purpose is defensive discipline, and the writing stays on that side of the line.