COMUNICATO STAMPA

Un difetto di programmazione nei dispositivi Coldcard: sottratti bitcoin per 70 milioni di dollari

Il difetto, presente da oltre cinque anni, ha reso vulnerabili le chiavi generate dagli hardware wallet del produttore Coinkite e ha permesso di prelevare i fondi senza mai toccare i dispositivi. L'attacco non risulta dipendere da errori operativi degli utenti. CheckSig: la sicurezza della custodia deve poter essere verificata da terze parti indipendenti.

Milano, 1 agosto 2026 — Il 30 luglio, in una finestra di 41 minuti, un attaccante ha svuotato 1.196 indirizzi Bitcoin per 1.082,65 BTC (circa 70 milioni di dollari) protetti da hardware wallet Coldcard, senza ricorrere a phishing, malware o accesso fisico ai dispositivi. Un difetto del firmware presente dal marzo 2021 ha *indebolito* la casualità con cui i dispositivi generavano il seed, il segreto crittografico da cui derivano le chiavi private, rendendo quelle chiavi ricostruibili a distanza. Coinkite, il produttore canadese, ha pubblicato un avviso di sicurezza dopo le prime segnalazioni dei prelievi, riconoscendo il difetto e distribuendo firmware correttivo, e ha precisato che l'aggiornamento non sana le chiavi già generate.

L'incidente

La causa non è un attacco crittografico ma un errore di implementazione: la generazione del seed prelevava casualità da una funzione software di riserva invece che dal generatore hardware di numeri casuali del dispositivo. Sull'origine della regressione le fonti divergono. L'avviso di Coinkite individua come vulnerabili i Mk3 dalla versione 4.0.1 alla 4.1.9; l'analisi indipendente di Block la fa risalire alla versione 4.0.0, pubblicata il 17 marzo 2021, e include nel proprio perimetro anche il Mk2, che l'avviso del produttore non nomina.

I bitcoin sottratti sono stati consolidati in pochi minuti su quattro indirizzi. Clay Garrett, di Block, ha dichiarato di aver individuato l'account a pagamento presso un noto fornitore di dati blockchain utilizzato dall'attaccante per interrogare gli indirizzi di origine durante i prelievi; i log interni del fornitore corrispondono al flusso di lavoro ipotizzato per numero, tempistica e sequenza delle richieste e le evidenze sono state trasmesse alle autorità.

«Sarà interessante seguire su blockchain le tracce di quanto trafugato: per nessuno sarà facile riciclare quei bitcoin. Sono somme rilevanti, la cui provenienza è pubblicamente documentata e associata a un evento noto, su indirizzi che l'intero settore sta monitorando; qualunque tentativo di immetterle in circolazione attraverso operatori regolamentati incontrerà controlli antiriciclaggio», osserva Ferdinando Ametrano, amministratore delegato di CheckSig.

Indicazioni per i possessori di Coldcard

Chi ha generato le proprie chiavi su firmware vulnerabile deve aggiornare il dispositivo, creare un nuovo seed, verificare il backup e un indirizzo di ricezione, inviare una transazione di prova e quindi trasferire il saldo residuo. Non esiste un test che, esaminando il solo seed, possa certificarne a posteriori l'entropia, e trasferire un seed debole su un altro dispositivo

non ne corregge la debolezza. Ledger ha dichiarato di non essere interessata dall'avviso, richiamando il generatore di numeri casuali certificato integrato nel proprio secure element; analoghe precisazioni sono state diffuse da Trezor, Block e altri produttori.

I limiti della custodia in autonomia

L'episodio riapre il confronto sui limiti della custodia gestita in autonomia dall'investitore.

«La self-custody trasferisce all'investitore il controllo, ma insieme al controllo rischi tecnici e operativi che spesso non è in condizione di osservare: "your keys, your coins" diventa allora "your keys, your problems". Il problema non è la custodia in autonomia, che deve sempre essere possibile, ma l'idea che il possesso delle chiavi equivalga automaticamente a sicurezza. Gli utenti colpiti non hanno sbagliato nulla, e la nostra solidarietà va a loro come a tutti i risparmiatori a cui si chiede di valutare ciò che non hanno le competenze per valutare. È ragionevole pretendere che quella valutazione sia fatta da terzi indipendenti e qualificati, e che sia documentata. Meglio quindi affidarsi a custodia professionale priva di singoli punti di rottura, con controlli documentati, verificati indipendentemente, e responsabilità contrattuali e coperture assicurative: non può eliminare tutti i rischi ma li governa efficacemente», commenta Ametrano.

L'entropia deve essere indipendente dal dispositivo

Coinkite ha segnalato che gli utenti che durante la configurazione avessero aggiunto almeno cinquanta lanci di dado indipendenti avrebbero ottenuto seed robusti nonostante il difetto: la casualità di origine esterna, combinata con quella del dispositivo, ne avrebbe compensato la debolezza. Nel prendere le distanze dall'incidente, anche Trezor ha indicato come propria salvaguardia la combinazione di più sorgenti indipendenti di casualità.

«L'entropia con cui si genera un seed non dovrebbe dipendere dal dispositivo che lo custodisce. Se il generatore interno al dispositivo è l'unica sorgente di casualità, diventa un punto singolo di rottura: un difetto ne indebolisce l'output senza che alcun controllo successivo possa rivelarlo, perché una chiave debole è indistinguibile da una robusta fino al momento in cui qualcuno la indovina. Non è un rischio teorico, è quanto è appena accaduto. Una procedura corretta combina entropia proveniente da sorgenti indipendenti dal dispositivo, all'interno di procedure formalizzate, con segregazione dei ruoli e controlli indipendenti sui relativi processi, come facciamo in CheckSig», spiega Paolo Mazzocchi, chief operating officer di CheckSig.

Il setup di custodia CheckSig

Nel setup di custodia di CheckSig, ogni dispositivo è inizializzato con entropia esterna e indipendente: la condizione che nell'incidente avrebbe protetto gli utenti che avessero aggiunto lanci di dado propri. L'infrastruttura impiega inoltre dispositivi di produttori diversi e combina firmware dei produttori con firmware proprietari: il difetto di una singola implementazione non può compromettere l'insieme delle chiavi.

Inoltre, nel protocollo di custodia di CheckSig, pubblico e documentato, nessuna singola chiave consente di disporre dei fondi: la sottoscrizione delle transazioni richiede tre distinti

stadi autorizzativi a firma multipla, per un totale di undici chiavi. Diversamente dalla firma singola, la firma multipla elimina l'esposizione on-chain delle informazioni crittografiche che un attaccante dovrebbe usare per risalire alle chiavi private. Tutti gli indirizzi colpiti nell'incidente erano infatti a firma singola.

In aggiunta, l'architettura frozen/cold a due livelli forza un primo trasferimento dal livello frozen a quello cold e prevede per il livello cold vincoli temporali (time lock) che impediscono il trasferimento immediato dei fondi, lasciando il tempo di rilevare un tentativo di sottrazione e di intervenire.

Infine, la prova-delle-riserve pubblica dimostra il controllo delle attività on-chain e la loro coerenza con le evidenze dichiarate; le attestazioni SOC 1 e SOC 2 Type II sono emesse a seguito di verifiche indipendenti sui controlli e sulla loro operatività nel periodo esaminato; le coperture assicurative aggiungono garanzie di ristoro.

In ogni caso, CheckSig non impiega il dispositivo interessato: nessuna delle chiavi in custodia è stata generata su un Coldcard. Anche in quel caso, tuttavia, i presidi descritti avrebbero operato indipendentemente dal difetto del firmware.

«Non promettiamo l'infallibilità di un dispositivo, di una chiave o di una persona: costruiamo una custodia in cui nessuno di questi elementi, da solo, è sufficiente a movimentare i fondi, in cui il cedimento di uno di essi può essere rilevato, e in cui i controlli sono documentati e verificati da soggetti indipendenti. La nostra è una promessa verificabile», conclude Ametrano.

Fonti

- Coinkite, avviso di sicurezza sulla generazione del seed: blog.coinkite.com
- Block, *Predictable RNG fallback and 32-bit reseed in Coldcard firmware*: engineering.block.xyz
- Galaxy Research, ricostruzione on-chain dei flussi: x.com/glxyresearch
- Clay Garrett (Block), tracciamento dell'operatore: x.com/clay_garrett
- Ledger, dichiarazione sui propri dispositivi: x.com/Ledger
- Chainalysis, analisi on-chain del 31 luglio: x.com/chainalysis
- Trezor, dichiarazione ai propri utenti del 31 luglio: x.com/trezor
- K33 Research, *Funds at risk: Coldcard's randomness flaw*: k33.com
- CheckSig: protocollo di custodia, prova-delle-riserve, attestazioni soc

CheckSig: eccellenza europea nei servizi per cripto-attività

Fondata nel 2019 come spin-off del Digital Gold Institute — il principale think tank europeo su Bitcoin, cripto-attività e blockchain — CheckSig è un Crypto Asset Service Provider (CASP) che offre soluzioni avanzate per investitori privati e istituzionali. La sua missione è rendere l'investimento in cripto-attività semplice e sicuro, offrendo servizi di acquisto e vendita, custodia, staking e supporto alla compliance fiscale. La società fornisce anche la piattaforma B2B / B2B2C CheckSig Clear (clear.checksig.com) ed è:

- *il primo CASP al mondo, dal 2020, ad aver introdotto la prova-di-riserva pubblica;*
- *il primo CASP ad aver ottenuto la licenza MiCAR in Italia;*
- *l'unico CASP italiano con copertura assicurativa — fornita da primaria compagnia con rating S&P AA;*
- *l'unico CASP italiano con attestazioni SOC 1 / SOC 2 Type II — ottenute per audit continui sui controlli di sistema e organizzativi condotti da una società appartenente alle Big Four;*
- *dal 2024, il primo operatore cripto ad agire come sostituto d'imposta per i clienti italiani.*

Contatti stampa: press@checksig.com