แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ Firmware ใน Coldcard Hardware Wallet

วันที่แจ้งเตือน 3 สิงหาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับช่องโหว่ ใน Coldcard Hardware Wallet ซึ่งอาจจะเชื่อมโยงกับเหตุการณ์ที่มีการขโมยเหรียญ Bitcoin

ช่องโหว่ดังกล่าวเกิดจากข้อผิดพลาดของ Firmware ส่งผลให้กระบวนการในการสร้าง Seed Phrase ไม่ได้ใช้ตัวสร้างเลขสุ่มหลัก (Random Number Generator: RNG) ที่ออกแบบไว้ ทำให้ชุด Seed Phrase ที่สร้างขึ้นมานั้นมีความอ่อนแอและคาดเดาได้ง่ายกว่าปกติ ทำให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ดังกล่าว คาดเดา Seed Phrase เพื่อเข้าถึง Wallet จาก Blockchain ได้ง่ายขึ้น ทั้งนี้ Firmware ที่มีความเสี่ยง ได้แก่ Mk2 หรือ Mk3 เวอร์ชัน 4.0.1 (March 2021) - 4.1.9 และ Mk4/Mk5 และ Q เวอร์ชันก่อนการอัปเดต Firmware

บริษัทผู้ผลิตได้เผยแพร่ Firmware ที่แก้ไขแล้ว ได้แก่ Mk2/Mk3: เวอร์ชัน 4.2.0 หรือใหม่กว่า, Mk4/Mk5 standard: เวอร์ชัน 5.6.0 หรือใหม่กว่า, Mk4/Mk5 Edge เวอร์ชัน 6.6.0X หรือใหม่กว่า, Q standard เวอร์ชัน 1.5.0Q หรือใหม่กว่า และ Q Edge: เวอร์ชัน 6.6.0QX หรือใหม่กว่า อย่างไรก็ดี การอัปเดต Firmware ไม่สามารถแก้ไข Seed Phrase ที่สร้างขึ้นก่อนการอัปเดตได้ ผู้ใช้งานที่อาจจะได้รับผลกระทบจึงควรสร้าง Seed Phrase ใหม่บน Firmware เวอร์ชันล่าสุด และโอนทรัพย์สินไปยัง Wallet ใหม่

เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว ผู้ใช้งานจึงควรพิจารณาตรวจสอบและอัปเดต Firmware Coldcard Hardware Wallet เป็นเวอร์ชันที่ได้รับการแก้ไขแล้ว และสร้าง Seed Phrase ใหม่บนอุปกรณ์ที่อัปเดตเป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต พร้อมตั้งค่า BIP-39 passphrase ที่มีความแข็งแรงและไม่ซ้ำกับที่ใช้งานอื่นเพื่อเพิ่มความมั่นคงปลอดภัย พร้อมทั้งตรวจสอบว่าไม่ได้ใช้อุปกรณ์ที่ได้รับผลกระทบในการ Sign (Signers) รวมถึงจัดเก็บ Seed Phrase และ Passphrase แยกจากกันในสถานที่ที่ปลอดภัย ไม่เปิดเผยต่อบุคคลอื่น และติดตามประกาศด้านความมั่นคงปลอดภัยจากผู้ผลิตอย่างสม่ำเสมอ

ข้อมูลอ้างอิง

1. https://blog.coinkite.com/coldcard-mk3-seed-generation-warning/
2. https://engineering.block.xyz/blog/predictable-rng-fallback-and-32-bit-reseed-in-coldcard-firmware
3. https://thehackernews.com/2026/08/coldcard-hardware-wallet-flaw-linked-to.html?m=1