01.April.2020

CoolWallet S Vulnerability Disclosure Status Update

This report provides an overview of how the CoolBitX Crypto app has been optimized based on the advice offered by Kraken. We'd like to thank the Kraken team for assessing the security of the CoolWallet S and raising these issues with us as part of their ethical disclosure process.

All the optimizations described below have now been deployed in our latest app version release and announced on public information channels (website, faq, etc.) of the product. In this status update, we discuss Kraken's findings, how we've successfully acted on this information, CoolWallet's security features as well as best practice measures that our users should employ.

Table of Contents

1. Summary

Kraken's security team periodically reviews the security of leading hardware wallets in order to improve the safety of their users' funds. In January 2020, Kraken Security Labs reached out to CoolBitX's technical team to inform us that they've assessed the CoolWallet S and identified potential vulnerabilities in the Android application. In accordance with their responsible disclosure policy, Kraken has afforded us the opportunity to investigate and address these issues.

As our community knows, the protection of our users' funds is our primary concern. While we hold the view that there have never been any substantial risks for CoolWallet S users, our development team has addressed these vulnerabilities and optimized the security of our application accordingly, to ensure the continued safety of your sensitive information. We explain

the steps we've taken in greater technical detail towards the end of this status update.

Kraken's report also allows us the opportunity to communicate with our community and reinforce best practice safety measures that our users should be employing. Specifically, we'll be discussing how to best protect your phone, card and recovery seed.

2. Kraken's Security Recommendations

Kraken informed us of the possibility that a user's PIN, pairing password and hardware seed information could be exposed to a skilled and sophisticated malicious actor if said party gains physical or remote access to both the user's phone and CoolWallet S by means of physical interception, malware infection or phishing techniques.

According to Kraken, an attacker can penetrate the CoolWallet's app by

1. either physically stealing your paired phone (which must have a disabled app PIN code)
2. or infiltrating it with malware that can record log data or take screenshots of sensitive information.

Kraken's team also considers it a vulnerability to carry both your CoolWallet S and paired phone on your person. Their team recommends the following actions to our users, to which we've added our thoughts:

1. **Update the CoolBitX Crypto Android app:**

As noted by Kraken, CoolBitx have released fixes in our latest app version that stops it from potentially disclosing the seed or AppLock PIN. We advise our users to always update to our latest official app releases as soon as possible.

2. **Generate your wallet seed on the CoolWallet S, not the app:**

While we provide our users with both options, we agree with Kraken and recommend that users should generate a seed with our card. This 2019 guide explains how and why.

3. **Turn on App Lock feature and display destination address**

We concur with Kraken- while it is not set as default options, it is helpful to enable these security features on our app. Our latest app release displays a notification that recommends this to users.

4. **Don't carry the CoolWallet S with a paired phone**

An essential part of the CoolWallet S' appeal is its slim dimensions that allow a user to discreetly carry it inside a conventional wallet. We designed the product with the intent to let our users access and transact their assets on-the-go. Kraken advises users not to carry a CoolWallet S with its paired phone on their person due to the risk of theft or robbery. We don't believe this security risk is any more severe than that facing USB-form hardware wallet users, who most likely leave their devices at home and not under their direct supervision most of the day. In fact, an affected CoolWallet S user will in all likelihood be alerted much faster to any possible theft or interception of their hardware wallet since they are likely to carry it on their person.

Ultimately it is the responsibility of each user to best ensure their personal safety. If in doubt whether a situation or location is safe, it's best not to carry a valuable item like your CoolWallet S, wallet or phone on your person to reduce the possibility of losing your phone and CoolWallet to the same person.

3. How CoolBitX secures the CoolWallet S

Over the past 5 years, CoolBitX has dedicated a substantial majority of our technical resources to strengthening and optimizing the security of our products - and we've taken a multi-layered process for securing the CoolWallet S, constantly improving to stay ahead of malicious actors. These measures include:

1. **EAL5+ Secure Element (private key protection)**

The Kraken report confirms the high level of certification of the CoolWallet's EAL5+ secure element (SE). This impenetrable microchip ensures that a user's private key is never compromised or revealed, not even to the user themself.

2. **Patented "Cold Compression" anti-tampering design**

Most established hardware wallets feature a USB form factor that has left them vulnerable to supply-chain and side-channel tampering, as documented by ethical hackers in the past. CoolWallet S’wafer-thin design and “Cold Compression" coating process makes it impossible for bad actors to tamper with the CoolWallet S without causing physical damage visible to the owner’s naked eye.

3. **2+1 Factor Authentication**

The CoolWallet S and app (iOS/Android) employ a unique 2+1 Factor Authentication process that combines several phone-based biometric and digital verification steps with a physical button confirmation after a visual check (wallet). This means that in a scenario where someone remotely manages to unlock your phone, they still need physical access to your card to transfer funds.

4. **Encrypted Bluetooth communication (AES256)**

The CoolWallet S uses a military-grade AES256 Bluetooth encryption to ensure wireless offline communication with our App. We have extensively tested and improved this resilience of this communication protocol since 2015. To our best knowledge, our Bluetooth communication remains secure and has yet to be compromised.

5. **AppLock PIN Code**

To further enhance security and privacy, we introduced an AppLock PIN code feature on the CoolBitX crypto app last year for users that desired additional peace of mind and privacy in regards to their portfolio details. We have recommended that our users utilize this feature to enhance their wallet security.

To unlock the CoolBitX Crypto app, you need to know your unique 6-digit code. You can also choose to deactivate or reset it as needed. For security reasons, CoolBitX does not keep any backup, and we therefore cannot assist in recovering a forgotten pin code. It is the user’s responsibility to determine how to store, protect, or whether to use this additional safety feature at all.

4. How to optimally secure your CoolWallet S

The Kraken assessment determines that the CoolWallet S' security is only as good as the safety measures that its owners take to protect their phone and recovery seed. We are in full agreement with this and have previously written extensively about how to best manage these areas. For our users' convenience, we'll do a quick recap here:

Seed Phrase Management

1. Make sure that you've securely backed up your seed phrase. Follow this guide if you're in doubt.
2. Generate your seed recovery by card, not our app. Write down your 12-24 seeds on our provided paper wallet and verify by checksum as prompted.
3. Store your recovery seed somewhere completely private and secure, and if possible, not in the same vicinity as your CoolWallet S
4. Never record or store your seed phrase or pairing pass in a digital format, such as a screenshot, photo or document.
5. Never reveal your seed phrase to anyone or if prompted by an email or phone call
6. Use our Advanced Seed Recovery feature if you need to restore your funds on a different CoolWallet S or mobile device.

In-App Security

7. Ensure you're using the latest CoolBitX Crypto app release version.
8. Ensure you've installed the official CoolBitX Crypto app from the Google Play (Android) or Apple App Store (iOS). Do not download from websites or sources provided by other parties.
9. Set a unique yet memorable 6-digit AppLock PIN code. Don't use your date of birth or a predictable sequence like 123456. Important: Do not attempt to set up a PIN if you haven't correctly backed up your seed recovery on your paper wallet. Forgetting your PIN without a backed-up recovery seed will likely result in you being permanently unable to access your funds.

Mobile Phone Security

10. Use your phone's biometric security measures such as fingerprint, facial recognition or pattern identification in conjunction with your phone's (unique) PIN code
11. Do not connect to unknown or suspicious WiFi connections in public
12. Do not engage with websites, applications, emails, messages or anything that may compromise your phone's security through malware or phishing methods.
13. Ensure that your phone's operating system and CoolBitX Crypto applications are up to date.
14. Check that your phone is not already compromised by malware.

Card Security

15. Only buy a CoolWallet S directly from us or a verified reseller.
16. Generate your recovery seed in private, via the card, not the app.
17. Visually confirm transaction details on the card's e-ink screen
18. Keep your CoolWallet S out of sight, and don't divulge its location or portfolio details to others
19. Know where your CoolWallet S is at all times.

5. Technical Response: Resolving Kraken's vulnerability issues

Sensitive data system logs and memory

As Kraken disclosed in the report, their team managed to uncover sensitive data such as the seed, pairing passphrase, and app PIN in logs and potentially in memory, which raises the risk of a successful device hack. In response, the CoolBitX technical team has made the changes described below to fix the issues.

1. We have disabled critical logs on the app in order to prevent the printing of logs with sensitive data
2. We applied security measures to the seed generation and PIN-related processes. As a result, malicious users cannot use third-party apps to record the screen or take screenshots when a user enters their seed or PIN.
3. We've completed our variables management optimization in order to speed up the process of memory garbage collection on sensitive data.

Transaction Detail Verification

The CoolWallet S has a feature that displays the transaction details, such as the receiving address and transaction amount, prior to the signing of the transaction. Prior to the Kraken report, this feature was not set as default.

In the latest release of the CoolBitX Crypto app, a new security alert informs users that a transaction's full details can optionally be displayed on their CoolWallet S. The notification will be displayed when the user first creates their wallet.

Warning for the risk of losing both card and phone and non-enabling of App Lock

To maximize security when using the CoolWallet S, please enable the passcode/ fingerprint/ facial recognition lock feature(s on your phone in conjunction with our AppLock feature for the CoolBitX Crypto application.

Also, be vigilant in how you physically protect and expose your phone and CoolWallet S. Failure to do so may result in the loss of your funds in the unlikely scenario that a third party gains simultaneous access to your phone and CoolWallet S.

If you have lost either your phone or CoolWallet S, please reach out to our customer support team who will advise you on how to restore access to your funds, or follow this guide.

App Lock

The latest released version of the CoolBitX Crypto app now features a 10-second timer that acts as a timeout function. Users are now required to confirm their identity with their unique 6-digit PIN if more than 10 seconds have elapsed between closing and returning to the app.

Avoid ADB Tool Hack

We have implemented a new approach to avoid executing the MainActivity directly. A prerequisite of verification is checked in MainActivity. Users who try to bypass the verification page will be redirected back to the initial verification process.

Transaction Authentication

According to the Kraken report, the transaction signature is designed without a authentication process. However, the CoolWallet S utilizes biometric verification on the mobile device as the authentication method.

PIN Code Storage

Third-party apps do not have access to the PIN if the device is not rooted or jailbroken. Also, the team managed to educate the users that rooted and jailbroken devices bring risk to their data security.

6. Conclusion

CoolBitX commenced work on the CoolWallet S in early 2015, building the first hardware wallet with a credit-card form factor and Bluetooth connectivity, and heralding in a new category of untethered and portable card-form hardware wallets in the process. Since then, the CoolWallet has navigated uncharted waters as we continued to iterate on our product and its evolving security.

We therefore view it as our responsibility to lead the development of safety benchmarks for mobile hardware wallets. CoolBitX welcomes penetration assessments from industry experts like Kraken Security Labs and we view their findings with an utmost sense of seriousness and urgency.

Based on Kraken's report, the team has satisfactorily optimized the security experience in the Android app and successfully closed the attack vectors that malicious users could potentially use to extract sensitive data stored in the app.

Some areas of concern, such as rooted and jailbroken devices, are beyond the control of our team and depend on the personal vigilance and responsibility of CoolWallet S users. That's why we have published guides and made public announcements to educate our users and urge them to secure their devices, for example by enabling the AppLock PIN in the CoolBitX Crypto app.

CoolBitX extends our warmest thanks to the Kraken Security Labs team for scrutinizing the resilience of the CoolWallet S's security processes in such great detail and for affording us the opportunity to act on their insights.

Providing such a fresh and expert perspective on possible attack vectors and device vulnerabilities are invaluable to our team and the community we serve.