A 15-year-old said he discovered vulnerability in hardware wallet

March 22 2018, by Nancy Owano

Headlines hummed with the discovery by a 15-year-old Saleem Rashid of a vulnerability he found in Ledger hardware wallets. He blogged about in on March 20.

What's Ledger and what are their hardware wallets? Ledger, said *Krebs on Security*, one of the numerous sites eyeing the teen's feat, is a

company whose products are designed to physically safeguard keys used to receive or spend the user's cryptocurrencies.

For example, the company describes its Ledger Nano S as "a Bitcoin, Ethereum and Altcoins hardware wallet, based on robust safety features for storing cryptographic assets and securing digital payments. It connects to any computer (USB) and embeds a secure OLED display to double-check and confirm each transaction with a single tap on its side buttons."

So, as Krebs explained, "Hardware wallets like those sold by Ledger are designed to protect the user's private keys from malicious software that might try to harvest those credentials from the user's computer. The devices enable transactions via a connection to a USB port on the user's computer, but they don't reveal the private key to the PC."

Is having private keys that can be connected to a PC via a USB port the perfect safeguard or the perfect storm? Anyone thinking about such a question was drawn to the blog posted by Rashid. He said an attacker could use the vulnerability to get private keys from the device.

Krebs reported that Kenneth White, director of the Open Crypto Audit Project, was impressed with Rashid's proof-of-concept attack code, which Rashid sent to Ledger approximately four months ago. (Saleem Rashid thanked Josh Harvey for providing him with a Ledger Nano S, to work on his exploit.)

Dan Goodin in *Ars Technica* presented an account of what Rashid did. He said the 15-year-old showed proof-of-concept code that allowed him "to backdoor" the Ledger Nano S hardware wallet.

John Biggs in *TechCrunch* noted that Ledger CEO Eric Larchevêque claimed that there were no reports of the vulnerability's effects on any

active devices. Joon Ian Wong, *Quartz*, similarly reported that Ledger said it was not aware of any funds that have been stolen from the devices."

Ledger officials, meanwhile, updated the Nano S to address the vulnerability. *Alphr* reported that Ledger issued a patch for the Ledger Nano S, four months after the initial disclosure. So as far as Nano S goes, Ledger said the problem was addressed.

The company blog posted on March 20, "Firmware 1.4: deep dive into three vulnerabilities which have been fixed," regarding "security improvements made to our firmware." They said they strongly encouraged their users to update their firmware by following their step by step guide.

According to Ledger, the firmware update patches three security issues. "The update process verifies the integrity of your device and a successful 1.4.1 update is the guarantee that your device has not been the target of any of the patched attack. There is no need to take any other action, your seed / private keys are safe."

Ledger has offices in Paris, Vierzon & San Francisco.

In the bigger picture, as many security pundits say, it is best not to assume any device is immune from attack.

Biggs in *TechCrunch* weighed in: "Ultimately, this breach shows us that hardware wallets are a good solution but still not foolproof. Regular updates and careful key management are still vitally important."

Quoted by *BBC News*, Craig Young, a researcher at security firm Tripwire, commented: "It is very difficult to thoroughly secure any device from attackers with physical access. This is why it is so critical to

have trusted component makers, merchants, and repair facilities."

More information: saleemrashid.com/2018/03/20/br … dger-security-model/

© 2018 Tech Xplore

Citation: A 15-year-old said he discovered vulnerability in hardware wallet (2018, March 22) retrieved 19 May 2024 from https://techxplore.com/news/2018-03-year-old-vulnerability-hardware-wallet.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.