Tester eyes unhackable claim on USB flash drive

May 12 2019, by Nancy Cohen

When the unhackable turns hackable you know there will be lots of noise. Case in point: The eyeDisk USB flash drive. Passwords exposed

in clear text were discovered.

ZDNet and numerous other sites were on the story by Friday. Researcher David Lodge, Pen Test Partners, found the level of security in eyeDisk did not match the claim.

"That's why we created eyeDisk, the world's first USB flash drive that uses iris recognition technology for unbeatable data security," its team had said. Also, they said, "eyeDisk can be used offline without any internet connection requirement and the software will not store or transmit your iris patterns, passwords, or any other information to any online location, ever. "

The device is relying on iris recognition. The project had raised funds on Kickstarter. UK-based Pen Test Partners, which does penetration testing, decided to examine eyeDisk's claims.

As it turned out, Pen Test Partners issued a vulnerability advisory on Thursday, posted by David Lodge.

"Last year, about the time we were messing around with a virtually unheard-of hardware wallet we got a bit excited about the word 'unhackable'. Long story short, I ended up supporting a selection of kickstarters that had the word 'unhackable or similar in their title."

Charlie Osborne, *ZDNet*, reported what happened when Lodge tried it out: "After plugging the eyeDisk into a Windows virtual machine (VM), the researcher found the product came up as a USB camera, a read-only flash volume, and a removable media volume." Osborne said it was possible " to obtain the password/hash, in clear text, by simply sniffing the USB traffic."

Lodge had picked, picked, picked apart components until reaching an

understanding: "What we have here is, literally, a USB stick with a hub and camera attached. That means most of the brains are in the software.

Lodge stated that "obtaining the password/iris can be achieved by simply sniffing the USB traffic to get the password/hash in clear text."

Zack Whittaker in *TechCrunch*: "Pen Test Partners researcher David Lodge found the device's backup password—to access data in the event of device failure or a sudden eye-gouging accident—could be easily obtained using a software tool able to sniff USB device traffic."

Lodge commented on "a very poor approach" given claims that it was unhackable. "The software collects the password first, then validates the user-entered password BEFORE sending the unlock password."

The flash drive is said to use iris recognition technology in tandem with AES-256 encryption.

What's next? Here is the timeline that Lodge provided. 9th April vendor acknowledges and advises they will fix – no date given; 9th April ask when they expect to fix, notify customers and pause distribution due to fundamental security issue. Advised public disclosure date 9th May 2019 – no response; 8th May final chase before disclosure; 9th May disclosed.

Hacking-weary sleuths would likely agree with Lodge's advice as the take-home. "Our advice to vendors who wish to make the claim their device is unhackable, stop, it is a unicorn."

More information: www.pentestpartners.com/securi … he-unhackable-again/

© 2019 Science X Network

Citation: Tester eyes unhackable claim on USB flash drive (2019, May 12) retrieved 19 April 2024 from https://techxplore.com/news/2019-05-tester-eyes-unhackable-usb.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.