Report finds uh-oh issues in popular password managers

February 22 2019, by Nancy Cohen

Credit: CC0 Public Domain

Vulnerabilities have been identified in password managers running on Windows 10. Maryland-based Independent Security Evaluators published a report earlier this week baring examination results on a number of popular password managers.

"In this paper we propose security guarantees password managers should offer and examine the underlying workings of five popular password managers targeting the Windows 10 platform," they said.

Scrubbing secrets from memory when they are not in use? That is what the authorities had initially anticipated would be the case in password managers. A "sanitization of memory once a password manager was logged out and placed into a locked state"? That is what they anticipated, too.

So what happened when they proceeded? They said that "trivial secrets extraction was possible from a locked password manager, including the master password in some cases."

Charlie Osborne in *ZDNet* summed up the findings, writing that "ISE was able to extract these passwords and other login credentials from memory while the password manager in question was locked."

PCWorld in 2017 defined a password manager as "an app that remembers your passwords for you and stores them in an encrypted vault. One master password unlocks the vault when you need to retrieve a password or create a new one, and does it without anyone being able to read what you type over your shoulder or track the login with a keylogger."

Osborne said in one example, "the master password which users need to use to access their cache of credentials was stored in PC RAM in a plaintext, readable format."

This would not be the first time that concerns have been raised about putting all your eggs in one basket. Neither will it be the last time you hear all the counter-arguments that, risk aside, it is still worth it to use a password manager that was carefully chosen.

PCWorld in 2017 is just one of many sites expressing the opinion that "despite issues of bugs and a market flooded with good and bad choices, security experts agree—a rarity—that password managers are the safest way for people to manage their accounts. The security benefits far outweigh the risks."

The Register in 2019 would agree to that, even with the findings in this recent report. "Password managers may leave your online crown jewels 'exposed in RAM' to malware – but hey, they're still better than the alternative." That was its headline earlier this week.

What is more, the security shortcomings that were revealed by ISE were described by *The Register* as "mildly annoying" and "non-world-ending."

That view resonates with what 1Password's security developer Jeffrey Goldberg told *PCMag* in an email. "The realistic threat from this issue is limited," he stated. "No password manager (or anything else) can promise to run securely on a compromised computer."

"The report doesn't by any means suggest you should not be using a password manager," said Nichols.

To be sure, the authors were quite clear that their findings did not support any conclusions that password managers were not only useless but also risky. "First and foremost," said the ISE authors, "password managers are a good thing. All password managers we have examined add value to the security posture of secrets management, and as Troy Hunt, an active security researcher once wrote, 'Password managers don't have to be perfect, they just have to be better than not having one."

Their intention in the paper was not "to criticize specific password manager implementations," but rather "to establish a reasonable minimum baseline which all password managers should comply with."

All in all, one is looking at a password manager issue of mainly "secure memory management."

Shaun Nichols in *The Register* saw a common thread among four password managers which left passwords – "either the master password or individual credentials – accessible in memory. This would potentially allow malware on a system, particular malware with admin rights, to obtain those passwords."

The report authors pointed out in their conclusions that "Each password manager also attempted to scrub secrets from memory. But residual buffers remained that contained secrets, most likely due to memory leaks, lost memory references, or complex GUI frameworks which do not expose internal memory management mechanisms to sanitize secrets."

Paul Lilly in *HotHardware* commented. "The takeaway seems to be that using a password manager is still wise, but there is room for improvement."

Threatpost, meanwhile, carried number of significant responses from password manager companies.

Sandor Palfy, CTO at LastPass, said the vulnerability highlighted by ISE was present in a "legacy" Windows application, and that the LastPass password manager has already received an update to minimize risk.

Emmanuel Schalit, CEO of Dashlane, said once the device is compromised, an attacker will end up having access to anything on the device and there is no way to effectively prevent it.

ISE had a number of recommendations, according to *PCMag*. Among their bits of advice were (1) use reputable antivirus products (2) shut down a password manager completely once you are done with it.

More information: Password Managers: Under the Hood of Secrets Management: www.securityevaluators.com/cas … ord-manager-hacking/

Citation: Report finds uh-oh issues in popular password managers (2019, February 22) retrieved 9 April 2024 from https://techxplore.com/news/2019-02-uh-oh-issues-popular-password.html