

Yes, this is NOT a real vulnerability. Neither CVE or NIST shows anything for KeePass 2.41; until something shows up here it's "unsubstantiated" aka like a "unpublished peer review".

■ **Other ways to display data (Score:2)**

by [Comboman \(895500 \)](#)

Keepass is basically as good as it can ever possibly be. The "vulnerability" they found relates to the fact that when it displays entries on screen Windows will make copies of some of the data to create the GUI, and there is no effective way to scrub that.

Are you kidding? That's easy, don't use system fonts to display the password on-screen. It takes a bit of effort to create letters from graphic elements like lines and semi-circles but it's much safer (/-\ = A, etc). You could even randomize the angles

■ **Re: (Score:2)**

by [GrandCow \(229565 \)](#)

The weak link is always the human.

If you're determined enough as a 3-letter agency to get in, then you can also disappear the person. Beat them enough and they'll give up the password. That beating can be either physically beating, or mental by doing things to family, friends, bank accounts, etc.

■ **Re: (Score:1)**

by [Cmdln Daco \(1183119 \)](#)

Translation: None of us should fret about this hyped up topic. Unless we are actors on the level where a government agency is going to come after us.

And no, few if any people on Slashdot meet that criterion. No matter how much we herp and derp about it.

■ **Re: (Score:2)**

by [Jeppe Salvesen \(101622 \)](#)

Or whoever established a foothold on a computer and is looking to expand their territory. Let's say they got something running from a drive-by infection. They can now proceed to access social media, buy stuff with the owner's money using amazon 1-click and so forth. Maybe even find the owner's actual comments on Pornhub in order to make the extortion mails more believable. Industrial espionage. Basically, these vulnerabilities can result in monetary gain for the attacker so it'll attract some proper talent.

■ **Re: (Score:2)**

by [Njovich \(553857 \)](#)

If you suspect the CIA/NSA is really after you I wouldn't recommend you to use Lastpass, or Windows. In fact your options are pretty limited and I would highly recommend to not get into that situation in the first place.

○ **Re: (Score:1)**

by [flirek \(1000761 \)](#)

Main memory of today's computers cannot be considered "private" & "secure" enough as Intel IME and similar garbage can directly read from it. Assumption that you have total control of memory is false.

○ **Re: (Score:2)**

by [cjeze \(596987 \)](#)

uh. it is absolutely not the bottom of the barrel. Most exploits works from inside the computer, if there are proven tools that can extract passwords and passphrases from memory it is just a matter of time before they can take over your whole life. If not fixed quickly exploits are going to pop up in the wild in 3..2..1..

■ **Re: (Score:1)**

by [msauve \(701917 \)](#)

Whoosh.

If a bad actor has control over a computer, they can simply use a keylogger. Way easier, and way less data to weed through.

WARNING! SECURITY ALERT! If someone has control of your computer, they have control of your computer.

[1 hidden comment](#)

○ **Re: (Score:3)**

by [scdeimos \(632778 \)](#)

Is it bottom of the barrel? I think it's healthy to stop and think about how password managers get used. If it makes you reconsider keeping your password manager open and unlocked all day every day, as opposed to only when you need it, this is a benefit. I'd never considered the implications of the Show/Hide Asterisks feature in KeePass, for example.

It's also important to remember: an attacker might have access to the memory of your computer, in which case you've lost the battle for your computer, but if th

■ **Re: (Score:1)**

by Anonymous Coward

Is it bottom of the barrel? I think it's healthy to stop and think about how password managers get used. ...

but if they can also score all your usernames and passwords as well, that really does give them the keys to the kingdom.

I'd say yes, at least with their keepass results, this is bottom of the barrel.

They say this is a vulnerability in keepass, yet the only place in ram they found plaintext keys was from the windows API.

That sounds to me like a windows problem and not a keepass problem.

All passwords are going to be used to authenticate to something. If you can only get at the plaintext key after it is handed off to that something, it does seem like a huge stretch to blame the password manager for it.

Or put another way, if yo

■ **Re: (Score:2)**

by [AmiMoJo \(196126 \)](#)

For most people the threat model they should be concerned with is password reuse and weak passwords. A password manager, even a flawed one, can fix both of those.

The convenience vs. security trade-off of not having to keep unlocking the password manager is worth it for most people, because the alternative is realistically going to be using "passw0rd" for everything. In fact I recommend people have their browser remember their passwords.

● **Re: (Score:2)**

by [Smidge204 \(605297 \)](#)

While true, that also means that it would have to wait until you actually copy/type the password in order to steal it, and there is still the task of identifying the password out of all the other data you copy or words you type through out the day.

Or, since you have access to the RAM, just snag it from the password manager whenever the process appears.

Then you get all the passwords at once, along with usernames or other important info, and you don't have to sift through junk data to find them.

=Smidge=

● **Not sure (Score:2)**

by [Artem S. Tashkinov \(764309 \)](#)

If I understand these two "vulnerabilities" properly, they require a piece of software installed/running locally which will steal/grab these passwords from RAM. However no normal/legitimate software will ever steal your passwords or access the RAM regions of other applications, which means this software is in essence malware which means you're already completely fucked and this software may just steal your master passwords, retrieve all files, etc. etc. etc.

○ **Re: (Score:2)**

by [mentil \(1748130 \)](#)

This could be relevant to memory-access attacks, like escaping from VMs, Docker containers etc.

It seems unlikely a server would be running a password manager app though.

■ **Re: (Score:2)**

by [Zocalo \(252965 \)](#)

It seems unlikely a server would be running a password manager app though.

No, but it's much more likely that a compromised PC with a password manager installed might be used to remotely log into that server and provide the attacker with a means to obtain the server's password. This provides another avenue of attack to obtain a server password, albeit perhaps not the easiest one to get the same results, but the more attack vectors there are the more likely it is that one will succeed, and it only takes on

■ **Re: (Score:2)**

by [Sique \(173459 \)](#)

It's not unlikely. Actually, it's quite often used.

Imagine an IT shop working remotely on diverse customer sites. There are dozens of technicians, and literally hundreds of passwords. One way to manage the password hell would be to assign a password safe to each customer, installed at the customer site on the server you use as central remote access. So your technician tasked with a job there would look up the password safe master key for that customer, and then remotely access the server there, to find th

○ **Re: (Score:3)**

by [Zocalo \(252965 \)](#)

There are varying degrees of "completely fucked", but yes, if you are being successfully attacked using this method then you are already in a pretty bad place, although it's possible that a lucky attacker might obtain enough info to pivot the attack onto an entirely separate system you happen to have a password for. Going from one PC being compromised to your entire network being compromised is definitely a step up in the level of "completely fucked".

Of course, if the malware has already been able to in

Re: (Score:2)
by [Kokuyo \(549451 \)](#)
I'd even go as far as to say that a relatively sophisticated keylogger is probably much easier to code and just as effective.

Use The Best Password (Score:2)
by [mentil \(1748130 \)](#)
That's why I always use a yuge password: 1234abcd. It's a very good password. The best password, really.

Re: (Score:3)
by [kbg \(241421 \)](#)
That's amazing! I've got the same combination on my luggage!


Re: (Score:2)
by [Opportunist \(166417 \)](#)
As long as the computer is off, it's also pretty secure in Lastpass and Keepass.

that's why I keep my passwords! (Score:2)
by [danbuter \(2019760 \)](#)
That's why I keep my passwords on a sticky note on my monitor! Never trust the cloud!

But we are still safe on (Score:2)
by [AHuxley \(892839 \)](#)
Apple? Thats all good right? And Linux? All good?

ugh (Score:2)
by [fluffernutter \(1411889 \)](#)
Independent Security Evaluators (ISE) published an assessment on Tuesday with the results of testing with several popular password managers.
I have to snicker that anyone would fail so spectacularly. They realized just now that memory has to hold field data at some point?

Related Links Top of the: day, week, month.
477 comments[Recruiters Are Still Complaining About No-Shows At Interviews](#)
445 comments[Should Developers Abandon Agile?](#)
441 comments[Hackers Who Attended Black Hat and DefCon Conferences Say Hotel Security Personnel Demanded Access To Their Rooms](#)
401 comments[Insect Collapse: 'We Are Destroying Our Life Support Systems'](#)
369 comments[China Infiltrated Apple, Amazon and Other US Companies Using Spy Chips on Servers, According To Bloomberg; Apple, and Amazon, Among Others Refute the Report](#)

[next](#)

[Montana Legislator Introduces Bills To Give His State His Own Science](#)
41 comments
[previous](#)


[NASA Eyes Colossal Cracks In Ice Shelf Near Antarctic Station](#)
39 comments

[Slashdot](#)
[Post](#)
[Get more comments](#)

64 of 64 loaded
[Submit Story](#)
How many QA engineers does it take to screw in a lightbulb? 3: 1 to screw it in and 2 to say "I told you so" when it doesn't work.
[FAQ](#)
[Story Archive](#)
[Hall of Fame](#)
[Advertising](#)
[Terms](#)
[Privacy Statement](#)
[Privacy Choices](#)
[Opt-out Choices](#)
[About](#)
[Feedback](#)
[Mobile View](#)
[Blog](#)

Trademarks property of their respective owners. Comments owned by the poster. Copyright © 2019 SlashdotMedia. All Rights Reserved.
[Close](#)

[Slashdot](#)
Working...