

Forum:[Hack Forums](#)

Thread: [Is TrueCrypt really defunct?](#)

Proposed - September 16, 2014, 7:12 pm

Hello, I recently went to re-install true crypt and found myself at a page redirecting me to BitLocker. Would it be wise to find an old True Crypt install and encrypt my hard drives or is there a security breach were the encryption can be broken otherwise defeating the purpose? Thanks for any and all information!

?A.J? - September 17, 2014, 3:38 am

They have ended the development of it, so every version is not secure and may contain unfixed security issues.

It'd be better if you use BitLocker.

FantaŠec - September 17, 2014, 3:42 am

<https://truecrypt.ch/>

Truecrypt ended due to unknown reasons. However, one of the reasons was not the lack of security. The security of it is still strong.

homeslice24 - September 23, 2014, 10:28 pm

Lol bitlocker.... go ahead use backdoor oem software

zombiesloth - September 24, 2014, 8:24 am

Truecrypt is still usable the header isn't as random as we all think but thats about the only real cryptographic issue. Other than that it's just not going to be worked on. In the years to come the whirlpool algo and other fast hashing algorithms will get faster to compute. So it is possible that they can be brute forced quicker even if you have a strong password since the 1000 iterations for sha or 2000 for whirlpool stays static. While that was a good way to slow down attacks back in 2008 but its 2014 now. AES isn't likely to have too many faults to be discovered in the future, but he inability to use stronger algorithms like sha512 (for full disk encryption) or more iterations on the hash makes it easier to break in the future.

tl;dr it's okay to use but it's like using a 2048 bit key for pgp. Still good at encryption because a key never goes bad unless it's stolen/cracked. It's good for now but don't continue to use it past 2016. You can use truecrypt for now until you find an alternative.

Ghanem - September 24, 2014, 8:40 am

I'm using veracrypt instead, that works good if you need an alternative. ?

Aura - October 1, 2014, 6:48 pm

OP, if you want I still have the original TrueCrypt 7.1a installer uploaded on mega if you want. Let me know if you need the link.

Also, the first result of the security audit being ran on it right now declared that version safe to use. We'll know for sure if TrueCrypt has been compromised or not in the next months, when the last communiqué will be released.