Secure Software Development (Computer Science) March 2022

Home / / My courses/ / SSDCS_PCOM7E March 2022 / / Unit 8 /

/ Collaborative Discussion 2: Cryptography case study: TrueCrypt / / Summary Post /

« Collaborative Discussion 2: Cryptography case study: TrueCrypt

Pavendran Wimalendran

Summary Post

12 days ago

1 reply

Last 3 days ago

FDE (full disk encryption) is a typical method of preventing unauthorised data access by encrypting the entire storage device. TrueCrypt is a well-known open-source tool that provides FDE. It supports many operating systems, including Windows, Mac OS, and Linux, and allows you to share encrypted storage between them (Q. -x. Miao, 2010). TrueCrypt was discontinued in 5/2014 owing to unresolved security problems and the end of support for Windows XP (TrueCrypt, 2014).

As a follow-up to my initial post below, and as suggested by my peers in their posts, I will also propose alternate solutions, such as VeraCrypt or BitLocker. It's also worth noting that TrueCrypt can still be utilised, which is preferable to having no protection at all, according to a number of my peers.

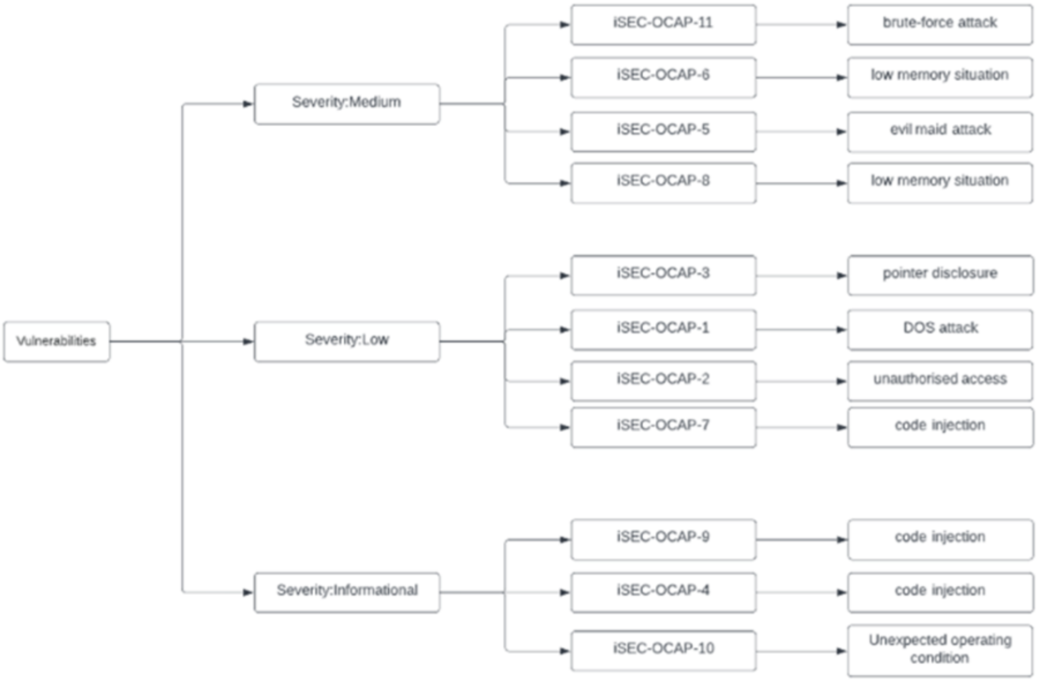
According to Junestam & Guigo (2014), 11 vulnerabilities were discovered (4 medium, 4 low, and 3 informational). Even while none of the vulnerabilities are severe/high, some of them are enough to conclude that TrueCrypt did not meet the necessary standards for secure coding.

For example, TrueCrypt uses a standard key derivation algorithm (PBKDF2) and relay on developers to specify an iteration count that influences the computational cost of deriving a key from a password. TrueCrypt uses either 1000 or 2000 iterations, depending on the hash function and use case. In all cases, the iteration count is insufficient to prevent even modestly complicated password guessing attempts.

If an attacker obtains access to an encrypted TrueCrypt volume and uses an offline brute-force and/or dictionary attack to recover the key used to encrypt the volume header, the volume can be decrypted.

Due to the above findings, as well as the fact that TrueCrypt has been discontinued since 2014, I would not recommend it to anyone.

Here is an ontology diagram that shows vulnerabilities by their severity and negative impacts on users.



References:

Junestam, A. & Guigo, N. (2014) Open Crypto Audit Project Truecrypt Security Assessment.Available from: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 7 May 2022]

Q. -x. Miao (2010), Research and analysis on Encryption Principle of TrueCrypt software system, *The 2nd International Conference on Information Science and Engineering*, 2010, pp. 1409-1412. Available from **https://ieeexplore.ieee.org/abstract/document/6824535** [Accessed 16 May 2022]

TrueCrypt (2014) Available from http://truecrypt.sourceforge.net/ [Accessed 16 May 2022]

Reply

1 reply

1

Post by **Sathira Padukka** **3 days ago**

Re: Summary Post

Great post, I agree with you on the alternate solutions, such as VeraCrypt or BitLocker. Because TrueCrypt contains some unfixed security issues.

The findings of iSEC team presented 11 different issues. Four of the issues are medium severity, four low severity and 3 informational severity issues. Some of these issues are in different classes, Cryptography, Data exposure, Data validation, Denial of service and Error reporting related to TrueCrypt. Anyways TrueCrypt was discontinued in 2014 and was replaced with VeraCrypt and other services.

Reply

Add your reply

Your subject

Type your post

Choose files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Summary Post

NEWER DISCUSSION

Summary Post