Secure Software Development (Computer Science) March 2022

« Collaborative Discussion 2: Cryptography case study: TrueCrypt

Pavendran Wimalendran

Initial Post

8 days ago

1 reply

Last 7 days ago

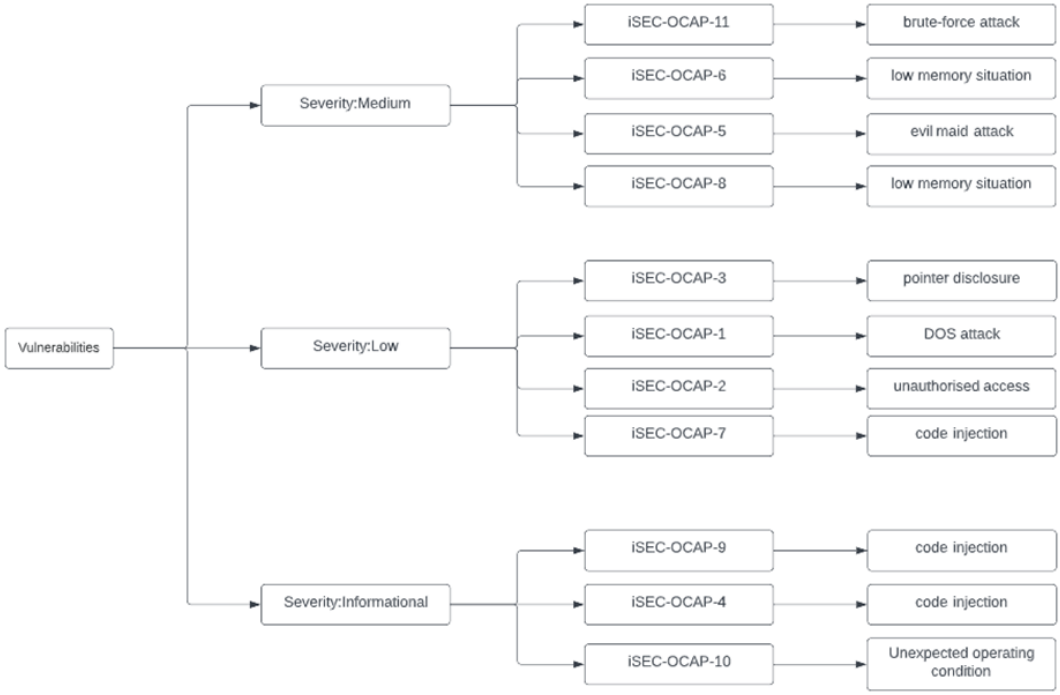
According to Junestam & Guigo (2014), 11 vulnerabilities were discovered (4 medium, 4 low, and 3 informational). Even while none of the vulnerabilities are severe/high, some of them are enough to conclude that TrueCrypt did not meet the necessary standards for secure coding.

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]

Reply

1 reply

1

Post by **Cathryn Peoples**
Re: Initial Post

7 days ago

Thank you very much, Pavendran. This is a very to-the-point response to the task set. Well done.

Best wishes,

Cathryn

Reply

Add your reply

Your subject

Type your post

Choose files No file chosen

Submit

Use advanced editor and additional options

Older discussion

Initial Post

Newer discussion

Initial Post