Is EFT vulnerable to the Raccoon attack?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

QUESTION

Is EFT vulnerable to the Raccoon attack?

ANSWER

No, if the Diffie-Hellman (DH) key exchange is disabled.

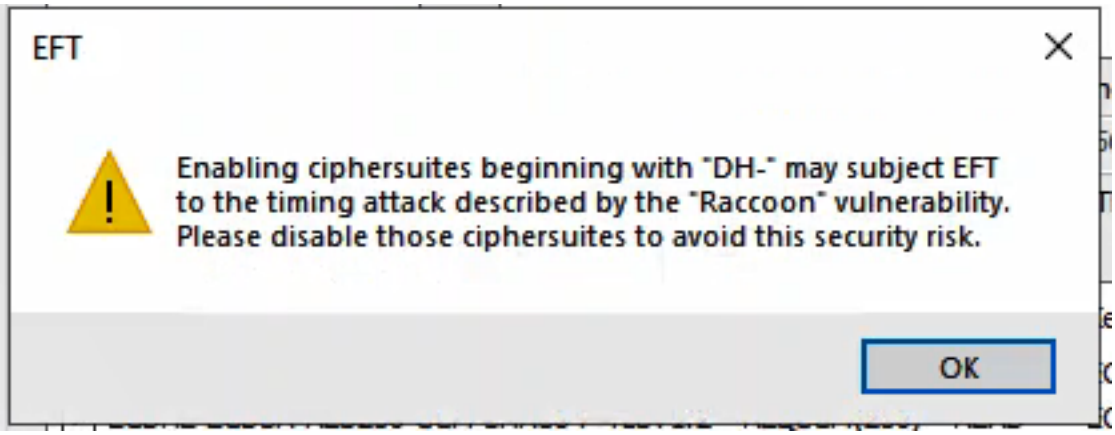
More Information

Raccoon is a timing vulnerability in the TLS specification that affects HTTPS and other services that rely on SSL and TLS. The attack generally targets the Diffie-Hellman (DH) key exchange in TLS 1.2 and below.

The OpenSSL 1.0.2 implementation reuses keys in cipher suites beginning with DH-. Only those are vulnerable. Not DH authentication, not DH key exchange etc. Only the specific combinations are vulnerable. That is, look at the cipher suite string; if it begins with DH-, the cipher suite is vulnerable. For example, DH-DSS-AES128-SHA256 is vulnerable.

For best security, disable ciphers that you do not need enabled.

If a cipher that begins with "DH-" is enabled, EFT will display the following warning:



Is EFT vulnerable to the Raccoon attack?

For more information about the Raccoon attack: https://raccoon-attack.com/

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11536/Is-EFT-vulnerable-to-the-Rac...