Is EFT affected by CVE-2015-4000 (AKA "Logjam")?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

QUESTION

Is EFT affected by CVE-2015-4000 (AKA "Logjam")?

ANSWER

No.

EFT provides COMPLETE control over ciphers and key exchange. We do not enable EXPORT ciphers by default. (If you have them enabled, you should disable them.)

For more information about this vulnerability and of Diffie-Hellman, refer to the following web pages:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
- Weak Diffie-Hellman and the Logjam Attack
- Guide to Deploying Diffie-Hellman for TLS

For more information about using SSH in EFT, refer to the help documentation.