Is EFT Server vulnerable to the CRIME attack on the SSL protocol?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, all versions

DISCUSSION

The CRIME attack is a recent vulnerability in the SSL protocol identified by researchers Juliano Rizzo and Thai Duong. This attack leverages an optional compression feature of the SSL protocol. Specifically, it uses the compression ratio of messages compressed by SSL to expose sensitive data such as session cookies.

The attack requires that the optional compression functionality of the SSL protocol be enabled. This compression feature is disabled within EFT Server and as such it is not vulnerable to this attack.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11096/Is-EFT-Server-vulnerable-to-...