Is EFT susceptible to the "Denial of service via recursive Deflate Stream" vulnerability?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.0.0.38 and 8.0.x
- This is fixed in EFT v8.1.0.16

QUESTION

Is EFT susceptible to the "Denial of service via recursive Deflate Stream" vulnerability?

ANSWER

Yes, you can be vulnerable if you are:

- Administering EFT remotely
- Allowing EFT remote administration to be initiated from the Internet
- Using the default port
- Not whitelisting trusted IPs

MORE INFORMATION

Sending a recursively compressed packet (a "quine") to the administration port can crash EFT. This can be mitigated by limiting access to administer EFT at the network level. You may be affected if you allow remote administration to EFT to be initiated from the internet. As stated in our best practices, do not expose port 1100 to the internet. You will always want to whitelist trusted IPs. The most secure method is to disallow remote administration outside of the host EFT server and only login in via localhost (::1 or 127.0.0.1).

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11588/Is-EFT-susceptible-to-the-De...