Is EFT susceptible to the "Authentication Bypass via Out-of-bounds Memory Read " vulnerability?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.0.x - 8.1.0.14
- This is fixed in v8.1.0.16

QUESTION

Is EFT susceptible to the "Authentication Bypass via Out-of-bounds Memory Read " vulnerability?

ANSWER

The possibility exists for malicious login attempts to eventually be mistaken as valid when a request is read beyond the payload buffer. Properly configured auto banning rules can avoid this type of attack. This is not a practical concern unless the administration port is exposed to external networks. This is even less of a concern if you are whitelisting expected IPs via the IP ban/access list for remote administration.

Yes, you can be vulnerable if you are:

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

MORE INFORMATION

This can be mitigated by limiting access to administer EFT at the network level. You may be affected if you allow remote administration of EFT to be initiated from the internet. As stated in our best practices, we do not recommend exposing port 1100 to the internet, but if you do, whitelist only trusted IP addresses. The most secure method is to disallow remote administration outside of the host EFT server and only login in via localhost, that is, ::1 or 127.0.0.1.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11586/Is-EFT-susceptible-to-the-Au...