Is EFT susceptible to the "Remotely obtain HDD serial number" vulnerability?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.0.0.38 - 8.1.0.14
- This issue will be addressed in a future release (not in a patch)

QUESTION

Is EFT susceptible to the "Remotely obtain HDD serial number" vulnerability?

ANSWER

An unauthenticated endpoint on EFT server returns a lightly-obfuscated base64 string that represents the numerical hard drive identifier. This is not a practical concern unless the administration port is exposed to external networks.

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 IP addresses

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 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 IP addresses. The most secure method is it 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/11589/Is-EFT-susceptible-to-the-Re...