Is EFT susceptible to the "Password Leak Due to Insecure Defaults" vulnerability?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

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

QUESTION

Is EFT susceptible to the "Password Leak Due to Insecure Defaults" vulnerability?

ANSWER

A researcher found that the default SSL setting was insecure for EFT v8.0.1.14.

MORE INFORMATION

For new installs, "Use SSL for secure remote administration" is enabled by default when allowing remote administration. It was verified that the admin credentials are not displayed when SSL is enabled. For upgrades, EFT will use the previously set settings for remote administration and SSL for administration and does not automatically change them when upgrading. (That is, if SSL was not enabled before you upgraded, it is not enabled after upgrading.) This vulnerability is configuration-based and heavily reliant on user configuration. Our best practices document outlines a recommendation to **always enable ssl for remote administration**. Additionally, to be affected by this, you would have had to remotely administer EFT from outside of the EFT server. As for any nonencrypted communication, if the user does not choose to use SSL, their communication can be inspected by nonauthorized parties.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11587/Is-EFT-susceptible-to-the-Pa...