Is EFT susceptible to the Zip Slip vulnerability?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.0.0.38 and 8.1.0.14
- This is fixed in v8.1.0.16

QUESTION

Is EFT susceptible to the Zip Slip vulnerability?

ANSWER

If you use the compression feature in our OpenPGP module, it is possible you are vulnerable. Our development team has mitigated the vulnerability in a new patch build.

MORE INFORMATION

ZIP Slip makes your application vulnerable to path traversal attacks and sensitive data exposure. This vulnerability was introduced by EFT's use of the /n compression library for OpenPGP module. Specially crafted malicious archives could deposit files in restricted folders using directory traversal, such as, a path that decompresses to ../../../malicious.zip.

WORKAROUND/SOLUTIONS

- Name files with standard names.
- Strip special characters from file names.
- Match and compare filenames with standard regular expressions.
- Rename all files in the uploaded zip with generated names before actually using/storing them
- It is recommended that if you are using EFT v8.0.0.38 to v8.1.0.14, you should upgrade to v8.1.0.16.

For more about naming files, refer to the following sources:

- Records Expires, from the Office of the Chief Records Office (OCRO) at the National Archives.
- Naming Files, Paths, and Namespaces, from Microsoft Learn

Is EFT susceptible to the Zip Slip vulnerability?

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11585/Is-EFT-susceptible-to-the-Zi...