PTC and WTC trigger security violations

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, v6.4 - 7.4.2.4 (Javascript code was removed in version 7.4.5.6)

SYMPTOM

PTC and WTC trigger security violations

RESOLUTION

To reduce the likelihood of these false alarms, the Javascript for the clients can be *minified* to remove comments.

MORE INFORMATION

Occasionally security scanners will flag certain key words used in Javascript comments as security violations for both the Plain Text Client (PTC) and the Web Transfer Client (WTC). Every effort has been made to remove anything in the source code that can cause spurious scanner hits. However, as scanners and browsers are updated and new scanners come onto the market, the PTC and WTC Javascript code may produce fresh false alarms. To reduce the likelihood of these false alarms the Javascript for the clients can be minified to remove comments and any spurious security hits associated with them.

The web client sources installed with EFT Server have not been minified, but EFT Server administrators can minify the code themselves. The tool YUI Compressor, version 2.4.7, has been used to remove comments from the WTC/PTC primary Javascript source files, and the resulting source code has been tested to ensure their behavior has not changed. Most Javascript minifiers will, by default, obfuscate the code in addition to removing comments and whitespace. If the purpose of the minification is to only remove comments, command line parameters can be used to turn off obfuscation. Here is an example usage of YUI Compressor that does not obfuscate the code:

```
java -jar yuicompressor-2.4.7.jar --nomunge --disable-optimizations
--line-break 0 EFTWebClientLogic.js -o EFTWebClientLogic-min.js
```

The above example demonstrates minifying the primary Javascript file for the WTC. The resulting file, EFTWebClientLogic**-min**.js, will be devoid of comments and whitespace, but

still mildly readable since no obfuscation was performed. It is a good idea to back up files before they are minified since once minified they cannot be restored.

To use this minified version of the file

1. In the folder from which the WTC/PTC is served, rename the current copy of the file (**EFTWebClientLogic.js**) to save it, in case you need to go back. For example, name it **EFTWebClientLogic_unmini.js**.
2. Copy the **-min** file into the folder and rename it to **EFTWebClientLogic.js**.
3. Open a browser and go to the WTC/PTC to see if you still get the security violations.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11102/PTC-and-WTC-trigger-security...