Enable or Disable Diffie-Hellman-group1-sha1 KEX for SFTP

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.2.1 - v7.3.6

NOTE: This registry setting is disabled as of EFT v7.3.7. This setting has been migrated to the EFT administration interface for EFT v7.3.7 and later. D*iffie-hellman-group-exchange-sha256* and *diffie-hellman-group14-sha1* are disabled by default. Refer to "*Configuring SFTP for a Site*" in the EFT help documentation for details of specifying SFTP advanced security options:

For EFT v7.3.7: **http://help.globalscape.com/help/eft7-3/#t=mergedProjects%2Fe**

DISCUSSION

In EFT version 7.2.1 -v7.3.6, the Diffie-Hellman-group1-sha1 KEX for SFTP is disabled by default to protect against the LOGJAM attack. Enabling the Diffie-Hellman-group1-sha1 KEX (with the LOGJAM vulnerability) will cause EFT to be non-compliant in PCI DSS v3.1 compliance scans. The DWORD value below is set to 0 (disabled) by default.

You can override the protection and enable the Diffie-Hellman-group1-sha1 KEX for SFTP to allow client compatibility (at the expense of being vulnerable to the LOGJAM attack and being non-compliant with PCI DSS v3.1 and later), by creating or editing the registry setting below and setting the DWORD value to 1 (enabled).

Create the following registry entry:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GlobalSCAPE Inc.\EFT Server 7.2

- Type: DWORD

Value name: SFTPEnableGroup1Kex

- Default Value: 0
- 0 = Disabled
- 1 = Enabled
- Cached: yes
- Backup/Restore: yes

Enable or Disable Diffie-Hellman-group1-sha1 KEX for SFTP

MORE INFORMATION

The following external articles might also be helpful:

- SSH Weak Diffie-Hellman Group Identification Tool: https://blog.gdssecurity.com/labs/2015/8/3/ssh-weak-diffie-hellman-group-identification-tool.html
- This tool establishes SSH connections to a server, thereby enumerating through various client configurations, in order to determine whether the server allows a Diffie-Hellman (DH) key exchange based on a weak group: https://github.com/GDSSecurity/SSH-Weak-DH
- A way to verify if certificate is configured correctly: https://www.ssllabs.com/ssltest/index.html

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11266/Enable-or-Disable-DiffieHell...