EFT and SSL Vulnerabilities

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

DISCUSSION

This notice is for informational purposes only and is intended to provide you with the latest update from Globalscape regarding the vulnerabilities in OpenSSL. On June 5, 2014, the Open SSL Foundation issued a warning about a new vulnerability in the open-source OpenSSL encryption protocol. CVE-2014-0224 (SSL/TLS MITM vulnerability) has been present in the code for 16 years and makes it possible for an attacker to conduct a man-in-the-middle attack on traffic encrypted with OpenSSL. EFT is minimally affected by the newly discovered vulnerability. Globalscape deems the risk posed by this issue to be low, but we strive to be transparent with any issues that may arise. We will be updating EFT's OpenSSL library to 0.9.8za in EFT version 7, which will be released the first week of July. In the meantime, we have issued private patch build 6.5.18.2 to mitigate this issue in all existing versions of EFT.

The following list will be updated with any new identified vulnerabilities or customer requests.

CVE-2014-0224	SSL/TLS MITM vulnerability	This vulnerability does affect EFT but the risk associated with this vulnerability is very low. The risk is low because the malicious Man In The Middle (MITM) attacker needs to have access to the communication channel to inject malicious payload with exact timing during the SSL handshake. Highly improbable to exploit, but we are working on upgrading to 0.9.8za to avoid this risk.

EFT and SSL Vulnerabilities

	CVE-2014-0221	DTLS recursion flaw	The EFT application is **not** vulnerable to this vulnerability as EFT does not implement DTLS.
	CVE-2014-0195	DTLS invalid fragment vulnerability	The EFT application is **not** vulnerable to this vulnerability as EFT does not implement DTLS.
	CVE-2014-0198	SSL_MODE_RELEASE_BUFFERS NULL pointer dereference	The EFT application is **not** vulnerable to this vulnerability as EFT uses OpenSSL 0.9.8t libraries; not OpenSSL 1.0.1
	CVE-2010-5298	SSL_MODE_RELEASE_BUFFERS session injection or denial of service	The EFT application is **not** vulnerable to this vulnerability as EFT uses OpenSSL 0.9.8t libraries; not OpenSSL 1.0.1
	CVE-2014-3470	Anonymous ECDH denial of service	This vulnerability affects EFT only if an EFT Admin has changed the default ciphers to include ECDH ciphers. Upon install of the EFT application, EFT defaults to the following SSL ciphers on the server side: AES256-SHA,CAMELLIA256-SHA,DES-CBC3-S
N/A		WTC Credentials are transferred to Server in Clear Text	Plaintext which seen in the browser dev tools is not yet network traffic, it is an HTTP datagram which is then passed through to the SSL layer before it gets to the TCP stack. This is showing the

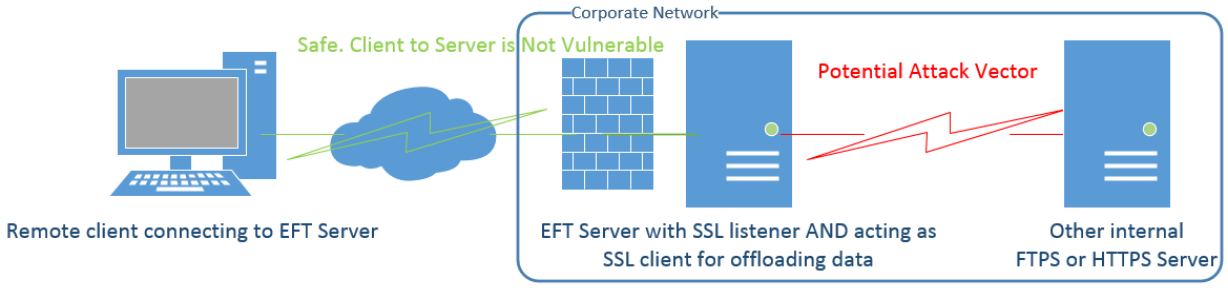
data before it is encrypted rather than when it is actually passed on to the server, so in this case it is not a security vulnerability.

.telerik-reTable-2 { BORDER-TOP: 0px solid; FONT-FAMILY: Tahoma; BORDER-RIGHT: 0px solid; BORDER-COLLAPSE: collapse; BORDER-BOTTOM: 0px solid; BORDER-LEFT: 0px solid } .telerik-reTable-2 TR.telerik-reTableHeaderRow-2 { FONT-SIZE: 11pt; BORDER-TOP: white 1pt solid; FONT-FAMILY: "Calibri" , "sans-serif"; BORDER-RIGHT: white 1pt solid; WIDTH: 119.7pt; BACKGROUND: #4f81bd; BORDER-BOTTOM: white 3pt solid; COLOR: #ffffff; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; MARGIN: 0in 0in 10pt; BORDER-LEFT: white 1pt solid; LINE-HEIGHT: 115%; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableHeaderFirstCol-2 { BORDER-TOP: white 1pt solid; BORDER-RIGHT: white 1pt solid; BORDER-BOTTOM: white 3pt solid; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; BORDER-LEFT: white 1pt solid; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableHeaderLastCol-2 { BORDER-TOP: white 1pt solid; BORDER-RIGHT: white 1pt solid; BORDER-BOTTOM: white 3pt solid; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; BORDER-LEFT: white 1pt solid; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableHeaderOddCol-2 { BORDER-TOP: white 1pt solid; BORDER-RIGHT: white 1pt solid; BORDER-BOTTOM: white 3pt solid; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; BORDER-LEFT: white 1pt solid; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableHeaderEvenCol-2 { BORDER-TOP: white 1pt solid; BORDER-RIGHT: white 1pt solid; BORDER-BOTTOM: white 3pt solid; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; BORDER-LEFT: white 1pt solid; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TR.telerik-reTableOddRow-2 { VERTICAL-ALIGN: top; COLOR: #666666; BACKGROUND-COLOR: #f2f3f4 } .telerik-reTable-2 TR.telerik-reTableEvenRow-2 { VERTICAL-ALIGN: top; COLOR: #666666; BACKGROUND-COLOR: #e7ebf7 } .telerik-reTable-2 TD.telerik-reTableFirstCol-2 { BORDER-TOP-STYLE: none; FONT-SIZE: 11pt; FONT-FAMILY: "Calibri" , "sans-serif"; BORDER-RIGHT: white 3pt solid; WIDTH: 119.7pt; BACKGROUND: #4f81bd; BORDER-BOTTOM-STYLE: none; COLOR: #ffffff; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; MARGIN: 0in 0in 10pt; BORDER-LEFT: white 1pt solid; LINE-HEIGHT: 115%; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableLastCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableOddCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableEvenCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TR.telerik-reTableFooterRow-2 { VERTICAL-ALIGN: top; COLOR: #666666;

EFT and SSL Vulnerabilities

PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt; BACKGROUND-COLOR: #ffffff } .telerik-reTable-2 TD.telerik-reTableFooterFirstCol-2 { BORDER-TOP-STYLE: none; FONT-SIZE: 11pt; FONT-FAMILY: "Calibri" , "sans-serif"; BORDER-RIGHT: white 3pt solid; WIDTH: 119.7pt; BACKGROUND: #4f81bd; BORDER-BOTTOM-STYLE: none; COLOR: #ffffff; PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; MARGIN: 0in 0in 10pt; BORDER-LEFT: white 1pt solid; LINE-HEIGHT: 115%; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableFooterLastCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableFooterOddCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt } .telerik-reTable-2 TD.telerik-reTableFooterEvenCol-2 { PADDING-BOTTOM: 0in; PADDING-TOP: 0in; PADDING-LEFT: 5.4pt; PADDING-RIGHT: 5.4pt }

Per the link provided below and the fact that the EFT application uses OpenSSL 0.9.8t and OpenSSL 0.9.8m (FIPS SSL) for all client and server secure file transfers, EFT is vulnerable to the SSL/TLS MITM vulnerability. However, please keep in mind that the attack vector requires the malicious man in the middle to have access to the communication channel between the two ends of the file transfer in order to inject malicious payload in a very carefully timed attack on the SSL handshake, leading this to be a very low risk threat for EFT.



Regarding the Anonymous ECDH denial of service vulnerability, EFT does NOT use ECDH ciphers by default. The EFT application defaults to the following SSL ciphers on the server side:

AES256-SHA,CAMELLIA256-SHA,DES-CBC3-SHA,AES128-SHA,IDEA-CBC-SHA,RC4-MD5,!EXP

As a result, it equates to enabling only the following cipher suites, in SSL/TLS specification nomenclature, in this order:

EFT and SSL Vulnerabilities

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_IDEA_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5

However, if an EFT Admin enables ECDH ciphers that override the SSL/TLS settings with "manually specified ciphers," they can reach out to our Support team and they will assist in verifying and disabling them.

Although the aforementioned vulnerabilities have little to no impact to the EFT application, please know that our Engineering team is working on a solution to address this issue. We should have a patch build available to address this issue soon. Please rest assured we are doing all we can to get in front of this issue.

If you would like more information on the new vulnerabilities in OpenSSL, please view the following link:

https://www.openssl.org/news/secadv_20140605.txt

If you have any further questions or concerns, please do not hesitate to contact Support.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11173/EFT-and-SSL-Vulnerabilities