The server issued one or more cookies that did not have the HttpOnly flag set

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, version 6.4.0 and later
- Mail Express, version 3.x and later

SYMPTOM

The server issued one or more cookies that did not have the HttpOnly flag set.

RESOLUTION

The server designates all cookies as HttpOnly where applicable; however, EFT Server's design requires that a certain number of its cookies be accessible by EFT Server's client side JavaScript; therefore, those cookies do NOT have the HttpOnly flag set.

You should also note that setting the HttpOnly flag does not guarantee that a cookie cannot be read by an attacker. Researchers have found at least one method to beat the HttpOnly flag using a technique called Cross Site Tracing (XST), which exploits the HTTP TRACE method. The good news is that EFT Server's HTTP engine does not support the TRACE method, thus rendering that particular attack vector nil (at least for those cookies protected by the HTTPOnly flag).

MORE INFORMATION

The purpose of the HttpOnly flag is to signify to the browser to not allow Javascript to access a particular cookie that contains sensitive information. Most commonly this is seen for a session cookie, because gaining this value will allow impersonating the user. Mail Express already uses the HttpOnly flag for the session cookie. Additional cookies are used; however, they don't contain sensitive information, just items to improve user experience. Also note that the HttpOnly flag does not guarantee that a cookie cannot be read by an attacker. Researchers have found attack vectors that can exploit it.

Cookies that do ***not*** have the HttpOnly flag set can be read by JavaScript. Should an XSS vulnerability exist on the site, an attacker could use JavaScript to read the session cookie and subsequently impersonate the user. The server administrator should continue to educate users on phishing and other scams that may result in an XSS type of attack. Prevention is the best cure in this case.

The server issued one or more cookies that did not have the HttpOnly flag set