TCP Sequence Number Approximation Vulnerability

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, all versions

SYMPTOM

A vulnerability and audit scan of our external web servers states that EFT Server has a "TCP Sequence Number Approximation Vulnerability"

RESOLUTION

To avoid this and other operating system vulnerabilities, you should regularly push the latest OS updates to each of your servers and desktop systems. The "TCP Sequence Number Approximation Vulnerability" is **not in EFT Server**, but in the operating system installed on the computer on which EFT Server is installed. Patches to Microsoft's operating systems have been released to address this issue. The Microsoft Security Bulletins linked below have links to the latest patches/updates.
For more information about the "TCP Sequence Number Approximation Vulnerability," please refer to the following links:

- Microsoft Security Bulletin MS05-019, "Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service": http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
- Microsoft Security Bulletin MS06-064, "Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service": http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
- Microsoft Security Updates: http://www.microsoft.com/downloads/en/results.aspx?displaylang=en&freetext=security%20update
- Sign up for Microsoft Download Notifications Newsletter: http://www.microsoft.com/downloads/en/DownloadNotifications.aspx

MORE INFORMATION

The Windows OS generates the TCP packets and PRNG sequence numbers (not EFT Server). The TCP protocol assigns an initial sequence number to each connection. Prior to updating the OS, it is possible, through careful analysis, to determine the initial TCP sequence number for a specific communications session. By predicting a TCP session's sequence number, it is possible to disrupt the integrity of a communication session that does not

provide its own session integrity. This is often referred to as "connection hijacking." EFT Server provides many protections such as flooding and denial of service prevention, controlling access by IP address, setting maximum connections per IP address, and others.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10589/TCP-Sequence-Number-Approxim...