U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Man-in-the-Middle Attacks and "HTTPS Inspection Products"

April 2017

Man-in-the-middle (MITM) attacks occur when a third party intercepts and potentially alters communications between two different parties, unbeknownst to the two parties. MITM attacks can be used to inject malicious code, intercept sensitive information like protected health information (PHI), expose sensitive information, and modify trusted information.

Many organizations have implemented end-to-end connection security on their internet transactions using Secure Hypertext Transport Protocol, or "HTTPS." Additionally, some organizations use "HTTPS interception products" to detect malware over an HTTPS connection. HTTPS interception products, also known as "HTTPS inspection," work by intercepting the HTTPS network traffic and decrypting it, reviewing it, then re-encrypting it. To do so, HTTPS interception products must install trusted certificates on client devices to perform the HTTPS inspection without presenting warnings.

However, this process may leave organizations using HTTPS interception products vulnerable, because the organizations can no longer verify web servers' certificates; view the protocols and ciphers that an HTTPS interception product negotiates with web servers, and, most importantly, independently validate the security of the end-to-end connection. In other words, the organizations that use these interception products are able to validate only the connection between themselves and the interception product, not between themselves and the server. This is problematic, because many HTTPS interception products do not properly verify the certificate chain before re-encrypting and forwarding information to the organizations, which leaves the connection vulnerable to a malicious MITM attack.

The United States Computer Emergency Readiness Team (US-CERT) recommends that organizations verify that their HTTPS interception product properly validates certificate chains and passes any warnings or errors to the client. Organizations can find a partial list of products that may be affected at CERT Coordination Center's The Risks of SSL Inspection. Also, organizations may use badssl.com as a method of determining if their HTTPS interception product properly validates certificates and prevents connections to sites using weak cryptography.

Securing end-to-end communications performs an important function in protecting the privacy of HTTPS traffic and preventing some forms of MITM attacks. US-CERT recommends reviewing the following mitigations in Alert TA15-120A to reduce vulnerability to MITM attacks:

- Update Transport Layer Security and Secure Socket Layer (TLS/SSL)
  US-CERT recommends upgrading TLS to 1.1 or higher and ensuring TLS 1.0 and SSL 1, 2, 3.x are disabled unless required. The continued use of TLS 1.0 and SSL 1, 2, 3.x is leading to increased cases affected by MITM attacks and session hijacks.

- Utilize Certificate Pinning
- Implement DNS-based Authentication of Named Entities (DANE)
- Use Network Notary Servers

Further, a recent security analysis (*The Security Impact of HTTPS Interception*) of HTTPS interception products found that poor implementation of many of these products may actually reduce end-to-end security and introduce new vulnerabilities. US-CERT recently issued an Alert, TA17-075A, warning of the vulnerabilities that organizations expose themselves to when they use HTTPS interception products.

Covered entities and business associates using HTTPS interception products or considering their use should consider the risks presented to their electronic PHI transmitted over HTTPS, and intercepted with an HTTPS interception products, as part of their risk analysis, particularly considering the pros and cons discussed by the US-CERT alerts, and the increased vulnerability to malicious third-party MITM attacks.

In addition to reviewing recommendations from US-CERT, covered entities and business associates should also review recommendations from the National Institute of Standards and Technology (NIST) for securing end-to-end communications, especially regarding the configuration, use and updating of TLS/SSL implementations. OCR's *Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* references NIST SP-800 series publications to describe the valid encryption processes to use to ensure that electronically transmitted PHI is not unsecured.

Resources:

US-CERT Alert TA15-120A, Securing End-to-End Communications
https://www.us-cert.gov/ncas/alerts/TA15-120A

The Security Impact of HTTPS Interception
https://jhalderm.com/pub/papers/interception-ndss17.pdf

US-CERT Alert TA17-075A, HTTPS Interception Weakens TLS Security
https://www.us-cert.gov/ncas/alerts/TA17-075A

CERT Coordination Center, The Risks of SSL Inspection
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

NIST SP 800-52 Rev. 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

HHS OCR Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html