Alert (TA17-075A)

HTTPS Interception Weakens TLS Security

Original release date: March 16, 2017

Systems Affected

All systems behind a hypertext transfer protocol secure (HTTPS) interception product are potentially affected.

Overview

Many organizations use HTTPS interception products for several purposes, including detecting malware that uses HTTPS connections to malicious servers. The CERT Coordination Center (CERT/CC) explored the tradeoffs of using HTTPS interception in a blog post called The Risks of SSL Inspection [1].

Organizations that have performed a risk assessment and determined that HTTPS inspection is a requirement should ensure their HTTPS inspection products are performing correct transport layer security (TLS) certificate validation. Products that do not properly ensure secure TLS communications and do not convey error messages to the user may further weaken the end-to-end protections that HTTPS aims to provide.

Description

TLS and its predecessor, Secure Sockets Layer (SSL), are important Internet protocols that encrypt communications over the Internet between the client and server. These protocols (and protocols that make use of TLS and SSL, such as HTTPS) use certificates to establish an identity chain showing that the connection is with a legitimate server verified by a trusted third-party certificate authority.

HTTPS inspection works by intercepting the HTTPS network traffic and performing a man-in-the-middle (MiTM) attack on the connection. In MiTM attacks, sensitive client data can be transmitted to a malicious party spoofing the intended server. In order to perform HTTPS inspection without presenting client warnings, administrators must install trusted certificates on client devices. Browsers and other client applications use this certificate to validate encrypted connections created by the HTTPS inspection product. In addition to the problem of not being able to verify a web server's certificate, the protocols and ciphers that an HTTPS inspection product negotiates with web servers may also be invisible to a client. The problem with this architecture is that the client systems have no way of independently validating the HTTPS connection. The client can only verify the connection between itself and the HTTPS interception product. Clients must rely on the HTTPS validation performed by the HTTPS interception product.

A recent report, The Security Impact of HTTPS Interception [2], highlighted several security concerns with HTTPS inspection products and outlined survey results of these issues. Many HTTPS inspection products do not properly verify the certificate chain of the server before re-encrypting and forwarding client data, allowing the possibility of a MiTM attack. Furthermore, certificate-chain verification errors are infrequently forwarded to the client, leading a client to believe that operations were performed as intended with the correct server. This report provided a method to allow servers to detect clients that are having their traffic manipulated by HTTPS inspection products. The website badssl.com [3] is a resource where clients can verify whether their HTTPS inspection products are properly verifying certificate chains. Clients can also use this site to verify whether their HTTPS inspection products are enabling connections to websites that a browser or other client would otherwise reject. For example, an HTTPS inspection product may allow deprecated protocol versions or weak ciphers to be used between itself and a web server. Because client systems may connect to the HTTPS inspection product using strong cryptography, the user will be unaware of any weakness on the other side of the HTTPS inspection.

Impact

Because the HTTPS inspection product manages the protocols, ciphers, and certificate chain, the product must perform the necessary HTTPS validations. Failure to perform proper validation or adequately convey the validation status increases the probability that the client will fall victim to MiTM attacks by malicious third parties.

Solution

Organizations using an HTTPS inspection product should verify that their product properly validates certificate chains and passes any warnings or errors to the client. A partial list of products that may be affected is available at The Risks of SSL Inspection [1]. Organizations may use badssl.com [3] as a method of determining if their preferred HTTPS inspection product properly validates certificates and prevents connections to sites using weak cryptography. At a minimum, if any of the tests in the Certificate section of badssl.com prevent a client with direct Internet access from connecting, those same clients should also refuse the connection when connected to the Internet by way of an HTTPS inspection product.

In general, organizations considering the use of HTTPS inspection should carefully consider the pros and cons of such products before implementing [1]. Organizations should also take other steps to secure end-to-end communications, as presented in US-CERT Alert TA15-120A [4].

Note: The U.S. Government does not endorse or support any particular product or vendor.

References

- The Risks of SSL Inspection
- The Security Impact of HTTPS Interception
- https://badssl.com/
- Securing End-to-End Communications

Revisions

- March 16, 2017: intial post