MS-ISAC™

Intel Byte
July 26, 2018, IB2018-0130
Information current as of July 20, 2018

TLS v1.2 Migration Impacting SLTT Governments

The MS-ISAC has high confidence that the industry move from the unsecure Transport Layer Security[1] (TLS) v1.0 and the seldom used v1.1 will have an increasing impact in the near future, forcing state, local, tribal, and territorial (SLTT) governments to migrate to TLS v1.2. The MS-ISAC recommends SLTT governments upgrade to TLS v1.2 in 2018 as outdated versions have known vulnerabilities that permit the interception and modification of data and are already being deprecated (discontinued) by vendors. As we expect the Internet Engineering Task Force (IETF) to announce TLS v1.3 within a year, SLTT governments should also begin developing TLS v1.3 implementation plans.

SLTT governments that do not upgrade to v1.2 are highly likely to experience compliance and service compatibility issues. As of June 30, 2018, the Payment Card Industry Data Security Standard (PCI DSS) no longer supports v1.0 and only support v1.1 configured per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 rev 1. At this time, SLTT government services that accept credit card payments and use outdated or misconfigured versions are not PCI compliant. Furthermore, Microsoft, Adobe, Cloud.gov, GitHub, IBM, and other vendors no longer support v1.0 or both v1.0 and v1.1, creating compatibility issues for associated services. Additionally, several certificate authorities, such as Digicert and Globalsign, are revoking certificates utilizing outdated versions, resulting in privacy warnings for end users attempting to connect to the websites. The Internet Engineering Task Force (IETF) also published a draft that outlines the potential deprecation of TLS v1.0 and v1.1, which would bring an official end to these versions.

Outdated versions of TLS, including v1.0 and its predecessor, Sockets Layer (SSL), insufficiently protect against a variety of cyber attacks, including Heartbleed, POODLE, BEAST, and FREAK, which have the ability to compromise the confidentiality and integrity of exchanged data. Furthermore, downgrade attacks capitalize on servers that still run outdated versions by forcing communication to occur over vulnerable versions of TLS/SSL.

The MS-ISAC advises SLTT governments to adhere to the following recommendations:

- Immediately update all services to TLS v1.2 and disable outdated TLS/SSL versions (including v1.1) if the service accepts credit card payments or connecting to vendors, certificate authorities, or others that only accept v1.2.
- After appropriate testing, ensure that clients and workstations web browsers are updated.
- If it is necessary to use v1.1, ensure the implementation follows NIST SP 800-52 rev 1.
- Where possible, plan to implement v1.3 by ensuring service and equipment purchases and upgrade plans incorporate it.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

[1] *TLS is a protocol that utilizes cryptography in order to secure data as it traverses the Internet during communication exchanges, such as those with web, email, file transfer protocol (FTP), voice over IP (VoIP), application programming interfaces (API), and virtual private network (VPN) servers.*