17.4. Transport Layer Security

Objective

17.4.1. Transport Layer Security is implemented correctly as an approved protocol.

Context

Scope

17.4.2. This section covers the conditions under which TLS can be used as an approved cryptographic protocols. Additionally, as File Transfer Protocol over SSL is built on SSL/TLS, it is also considered within scope.

17.4.3. When using a product that implements TLS, requirements for using approved cryptographic protocols will also need to be referenced in the Section 17.3 - Approved Cryptographic Protocols.

17.4.4. Further information on handling TLS traffic through gateways can be found in Section 14.3 - Web Applications.

Background

17.4.5. **Secure Sockets Layer (SSL)**, and **Transport Layer Security (TLS)** are cryptographic protocols designed to provide communication security when using the Internet. They use X.509 certificates and asymmetric cryptography for authentication purposes. This generates a session key. This session key is then used to encrypt data between the parties.

17.4.6. Encryption with the session key provides data and message confidentiality, and message authentication codes for message integrity.

17.4.7. Several versions of the SSL and TLS protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP).

17.4.8. Although common usage has been to use the terms TLS and SSL interchangeably, they are distinct protocols.

17.4.9. TLS is an Internet Engineering Task Force (IETF) protocol, first defined in 1999, updated in RFC 5246 (August 2008) and RFC 6176 (March 2011). It is based on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator web browser. A draft of TLS 1.3 was released in October 2014, with a definitive version issued in 2018.

17.4.10. Microsoft announced in October 2014 that that it will disable Secure Sockets Layer (SSL) 3.0 support in its Internet Explorer browser and in its Online Services, from Dec. 1, 2014.

SSL 3.0 Vulnerability

17.4.11. A design vulnerability has been found in the way SSL 3.0 handles block cipher mode padding. The Padding Oracle On Downgraded Legacy Encryption (POODLE) attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from an encrypted transaction.

17.4.12. The POODLE attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios. All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable.

SSL Superseded

17.4.13. SSL is now superseded by TLS, with the latest version being TLS 1.3 which was released in August 2018. This is largely because of security flaws in the older SSL protocols.

17.4.14. Accordingly SSL is no longer an approved cryptographic protocol and it SHOULD be replaced by TLS.

References

17.4.15. Further information on SSL and TLS can be found at:

Reference	Title	Publisher	Source
	The SSL 3.0 specification	IETF	https://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
RFC5246	**The TLS 1.2 specification**	IETF	https://tools.ietf.org/html/rfc5246
RFC6176	**The SSL 2.0 prohibition**	IETF	https://tools.ietf.org/html/rfc6176
RFC8446	**The Transport Layer Security (TLS) Protocol Version 1.3**	IETF	https://tools.ietf.org/html/rfc8446
	Vulnerability Summary for CVE-2014-3566	NIST	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
TA14-290A	**Alert (TA14-290A) - SSL 3.0 Protocol Vulnerability and POODLE Attack**	US-CERT	https://www.us-cert.gov/ncas/alerts/TA14-290A
	This POODLE Bites: Exploiting The SSL 3.0 Fallback	Google September 2014	http://www.openssl.org/~bodo/ssl-poodle.pdf [PDF, 213 KB]

Rationale & Controls

Using TLS

17.4.16.R.01. **Rationale**

Whilst version 1.0 of SSL was never released, version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS with the latest version being TLS 1.3 which was released in August 2018. SSL is no longer an approved cryptographic protocol.

17.4.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2598]

Agencies SHOULD use the current version of TLS (version 1.3).

17.4.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:2600]

Agencies SHOULD NOT use any version of SSL.