SSL/TLS 1.0 Vulnerability Response

SAFE Compliance Architecture Guide Supplement

CONTENTS

Abstract

This paper is a response to SSL/TLS 1.0 vulnerabilities of 2014. It provides guidance on addressing these vulnerabilities within Cisco products.

Background

In 2014, improved attacks such as the Heartbleed bug severely compromised the capability of older encryption technology to protect information. Secure Sockets Layer (SSL) and early forms of Transport Layer Security (TLS) no longer meet minimum security standards because of vulnerabilities in these protocols for which there are no fixes. Updates to infrastructure are necessary to protect information and meet today's compliance requirements.

Many compliance mandates reference NIST standards, including PCI, HIPAA, FIPS, Common Criteria, and so on. NIST SP 800-52 rev 1 provides updated guidance on secure TLS configurations and recommends migration to TLS 1.2.

Similarly, the PCI Security Standards Council (PCI SSC) announced the release of PCI DSS v3.1. This update was prompted by the broader security industry's conclusion that SSL version 3.0 and TLS 1.0 are no longer secure protocols. Therefore, these protocols can no longer be used after June 30, 2016 for systems that carry or manage credit card information. The PCI Council directs that support for SSL 3.0 and TLS 1.0 must be completely removed, and then preferably transition everything to TLS 1.2.

Organizations using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they do not already exist.

Overview

The Cisco Compliance Solution presents a PCI, HIPAA, and SOX audited reference design for achieving compliance in an organization. This paper supplements those Cisco Validated Designs by providing updated information on products and software that includes the ability to implement TLS 1.2 and help organizations maintain compliance.

The product list includes a subset of Cisco products based on those originally audited in the Cisco Compliance Solution Cisco Validated Designs.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

TLS 1.2 Capable Products

Table 1 lists the products, and their recommended replacements, which support TLS 1.2 for secure remote management and administration.

Table 1 Products and TLS Capability

Product	Software Version	TLS 1.2 Capable	End of Life	Replacement Product
Cisco Unified Communications Manager	10.5(2)	YES	NA	NA
Cisco UCS Manager	3.1 or 2.2.7MR6	YES	NA	NA
UCS Express	2.0.2	NO	7/31/2013	Cisco UCS E-Series
UCS E-Series	3.1 or 2.2.7MR6	YES	NA	NA
UCS B and C-Series	3.1 or 2.2.7MR6	YES	NA	NA
Cisco Secure Access Control Server	5.8	NO	NA	Cisco Identity Service Engine
Cisco Identity Service Engine	2.0	YES	NA	NA
Cisco Prime LMS	4.2.5	NO	11/30/2015	Cisco Prime Infrastructure (LMS is a component of PI now)
Cisco Prime Infrastructure	3	YES	NA	NA
Cisco Security Manager	4.7 SP2+	YES	NA	NA
CISCO3945	15.5.3(M)	YES	NA	NA
Cisco 4000 ISR	3.13.3S	YES	NA	NA
ASR 1002 (RP1)	3.16.0S	YES	NA	ASR 1002-X
ASR 1002-X (excludes SSL VPN)	3.16.0S	YES	NA	NA
Catalyst 4507R w/ Supervisor 7	NA	NO	7/31/2015	Catalyst 4507R+E
Catalyst 4507R+E w/ Supervisor 7E	3.7.2E	NO	NA	NA
Catalyst 6509 W/ SUP720-3BXL	15.1(1)SY	NO	1/31/2018	Planned for release 15.3(2)SY
Cisco Nexus 1000V	5.2(1)SV3(1.4)	YES	NA	NA
Cisco Nexus 7010 Chassis (“Supervisor module-1X”)	7.2(0)D1(1) (no WEB mgmt)	NA	8/31/2019	Cisco Nexus 7010 /w Sup2 Bundle
Cisco WCS Manager (Wireless Control System)	WCS 7.0.240.0	NO	5/31/2018	Cisco Prime Infrastructure
AIR-CT5508-12-K9	8.2	YES	NA	NA
AIR-CT5760	8.2	YES	NA	NA
MSE 3350	7.3.101.0(ED)	NO	9/30/2016	MSE 3355
MSE 3355	10.2	YES	6/30/2020	MSE 3365

Table 1 Products and TLS Capability (continued)

MSE 3365	10.2	YES	NA	NA
Wireless Access Points-Autonomous	15.3.3-JBB5(ED)	NO	NA	Add Controllers
Wireless Access Points-Controller	8.3 DTLS 1.2	YES	NA	NA
MDS 9506 (“Supervisor/Fabric-2”)	NX-OS 6.2(13a) (no WEB mgmt)	NA	NA	NA
Cisco ASAv	9.3.2	YES	NA	NA
Cisco ASA5515-X	9.3.2	YES	NA	NA
Cisco ASA5585-x	9.3.2	YES	NA	NA
WS-SVC-ASA-SM1	9.4.1	YES	NA	NA
Nexus VSG	5.2.1	NO	NA	Cisco ASAv
WS-SVC-IDSM-2	7.0(9)E4	NO	5/31/2018	FirePOWER Appliance/Services
IPS 4500	7.3(4)E4	YES	4/30/2020	FirePOWER Appliance/Services
FirePOWER 7000/8000 Series	5.4.0	YES	NA	NA
Firepower 9300 Series (ASA code)	9.4.1	YES	NA	NA
FireSIGHT Management Center	5.4.0	YES	NA	NA

References

- Cisco Compliance Solutions Cisco Validated Designs—www.cisco.com/go/compliance
- NIST SP 800-52 rev 1—http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
- PCI Compliance—https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
- Cisco’s Recommendations for Cryptographic Algorithms—http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html