Avoid the POODLE and POODLE BITES Vulnerability When You Use ASA and AnyConnect

Contents

Introduction

This document describes what you must do to avoid the Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability when you use Adaptive Security Appliances (ASAs) and AnyConnect for Secure Sockets Layer (SSL) connectivity.

Background Information

The POODLE vulnerability affects certain implementations of the Transport Layer Security version 1 (TLSv1) protocol and could allow an unauthenticated, remote attacker to access sensitive information.

The vulnerability is due to improper block cipher padding implemented in TLSv1 when you use Cipher Block Chaining (CBC) mode. An attacker could exploit the vulnerability in order to perform an "oracle padding" side-channel attack on the cryptographic message. A successful exploit could allow the attacker to access sensitive information.

Problem

The ASA allows incoming SSL connections in two forms:

1. Clientless WebVPN
2. AnyConnect Client

However, none of the TLS implementations on the ASA or the AnyConnect client are affected by POODLE. Instead, the SSLv3 implementation is affected so that any clients (browser or AnyConnect) that negotiate SSLv3 are susceptible to this vulnerability.

> **Caution**: POODLE BITES does however affect the TLSv1 on the ASA. For more information on affected products and fixes, refer to CVE-2014-8730.

Solution

Cisco has implemented these solutions to this problem:

1. All versions of AnyConnect that previously supported (negotiated) SSLv3 have been deprecated and the versions available for download (both v3.1x and v4.0) will not negotiate SSLv3 so they are not susceptible to the issue.

2. The ASA's default protocol setting has been changed from SSLv3 to TLSv1.0 so that as long as the incoming connection is from a client that supports TLS, that is what will be negotiated.

3. The ASA can be manually configured to accept only specific SSL protocols with this command:

   ```
   ssl server-version
   ```

   As mentioned in solution 1, none of the currently supported AnyConnect clients negotiate SSLv3 anymore, so the client will fail to connect to any ASA configured with either of these commands:

   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   However, for deployments that use the v3.0.x and v3.1.x AnyConnect versions that have been deprecated (which are all AnyConnect build versions PRE 3.1.05182), and in which SSLv3 negotiation is specifically used, the only solution is to eliminate the use of SSLv3 or consider a client upgrade.

4. The actual fix for POODLE BITES (Cisco bug ID CSCus08101) will be integrated into the latest interim release versions only. You can upgrade to an ASA version that has the fix to solve the problem. The first available version on Cisco Connection Online (CCO) is Version 9.3(2.2).

   The first fixed ASA software releases for this vulnerability are as follows:
   8.2 Train: 8.2.5.558.4 Train: 8.4.7.269.0 Train: 9.0.4.299.1 Train: 9.1.69.2 Train: 9.2.3.39.3 Train: 9.3.2.2

TLSv1.2

- The ASA supports TLSv1.2 as of software version 9.3(2).
- AnyConnect Version 4.x clients all support TLSv1.2.

This means:

- If you use Clientless WebVPN, then any ASA that runs this version of software or higher can negotiate TLSv1.2.

- If you use the AnyConnect client, in order to use TLSv1.2, you will need to upgrade to Version 4.x clients.

Related Information

  - CVE-2014-8730
  - Cisco bug ID CSCug51375
  - Cisco bug ID CSCur42776
- Technical Support & Documentation - Cisco Systems