使用ASA和AnyConnect时，避免POODLE和POODLE BITES漏洞

目录

简介

本文档介绍在使用自适应安全设备(ASA)和AnyConnect for Secure Sockets Layer(SSL)连接时，为避免Padding Oracle On Detraded Legacy Encryption(POODLE)漏洞，必须采取哪些措施。

背景信息

POODLE漏洞影响传输层安全版本1(TLSv1)协议的某些实施，并可能允许未经身份验证的远程攻击者访问敏感信息。

此漏洞是由于在使用密码块链(CBC)模式时在TLSv1中实施了不正确的块密码填充。攻击者可以利用此漏洞对加密消息执行“oracle padding”侧通道攻击。成功利用此漏洞可让攻击者访问敏感信息。

问题

ASA允许以两种形式传入SSL连接：

1. 无客户端WebVPN
2. AnyConnect Client

但是，ASA或AnyConnect客户端上的所有TLS实施均不受POODLE影响。相反，SSLv3实施会受到影响，因此协商SSLv3的任何客户端（浏览器或AnyConnect）都容易受到此漏洞的影响。

> **警告：**但是，POODLE BITES会影响ASA上的TLSv1。有关受影响产品和修复程序的详细信息，请参阅CVE-2014-8730。

解决方案

思科已针对此问题实施了以下解决方案：

1. 以前支持（协商）SSLv3的所有AnyConnect版本均已弃用，可供下载的版本（v3.1x和v4.0）将不会协商SSLv3，因此它们不易受此问题影响。

2. ASA的默认协议设置已从SSLv3更改为TLSv1.0，因此只要传入连接来自支持TLS的客户端，即会协商。

3. 可以使用以下命令手动配置ASA，以仅接受特定SSL协议：

   ssl server-version

   如解决方案1所述，当前支持的AnyConnect客户端不再协商SSLv3，因此客户端将无法连接到使用以下任一命令配置的任何ASA:

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

   但是，对于使用已弃用的v3.0.x和v3.1.x AnyConnect版本(所有AnyConnect构建版本都为VER 3.1.05182)且专门使用SSLv3协商的部署，唯一的解决方案是避免使用SSLv3或考虑客户端升级。

4. POODLE BITES(思科漏洞ID CSCus08101)的实际修复将仅集成到最新的中期版本。您可以升级到具有解决问题的修复的ASA版本。思科在线连接(CCO)上的第一个可用版本是9.3(2.2)版。

   此漏洞的第一个固定ASA软件版本如下：
   8.2火车： 8.2.5.558.4火车： 8.4.7.269.0火车： 9.0.4.299.1火车： 9.1.69.2火车： 9.2.3.39.3火车： 9.3.2.2

TLSv1.2

- 自软件版本9.3(2)起，ASA支持TLSv1.2。
- AnyConnect版本4.x客户端都支持TLSv1.2。

这意味着：

- 如果使用无客户端WebVPN，则运行此软件版本或更高版本的任何ASA都可以协商TLSv1.2。
- 如果使用AnyConnect客户端，为了使用TLSv1.2，您需要升级到版本4.x客户端。

相关信息

- CVE-2014-8730
- 思科漏洞ID CSCug51375
- 思科漏洞ID CSCur42776
- 技术支持和文档 - Cisco Systems