使用ASA和AnyConnect時避免POODLE和POODLE BITES漏洞

目錄

簡介

本文檔介紹在使用自適應安全裝置(ASA)和安全套接字層(SSL)連線的AnyConnect時，必須如何避免填充Oracle On Downgraded Legacy Encryption(POODLE)漏洞。

背景資訊

POODLE漏洞會影響傳輸層安全版本1(TLSv1)協定的某些實現，並且可能允許未經身份驗證的遠端攻擊者訪問敏感資訊。

此漏洞是由於使用密碼塊連結(CBC)模式時，在TLSv1中實現的塊密碼填充不正確造成的。攻擊者可以利用該漏洞對加密消息執行「oracle padding」旁通道攻擊。成功利用此漏洞可使攻擊者訪問敏感資訊。

問題

ASA允許以兩種形式傳入的SSL連線：

1. 無客戶端WebVPN
2. AnyConnect客戶端

但是，ASA或AnyConnect客戶端上的任何TLS實現都不受POODLE影響。相反，SSLv3實施會受到影響，因此協商SSLv3的任何客戶端（瀏覽器或AnyConnect）都容易受到此漏洞的影響。

> **注意**：但是，POODLE BITES會影響ASA上的TLSv1。有關受影響產品和修復程式的詳細資訊，請參閱CVE-2014-8730。

解決方案

思科已針對此問題實施以下解決方案：

1. 先前支援（協商）SSLv3的所有版本的AnyConnect都已棄用，且可供下載的版本（v3.1x和

v4.0）不會協商SSLv3，因此它們不會受到此問題的影響。

2. ASA的預設協定設定已從SSLv3更改為TLSv1.0，因此只要傳入連線來自支援TLS的客戶端，即將協商的協定。

3. 使用以下命令，可以手動將ASA配置為僅接受特定的SSL協定：

   ssl server-version

   如解決方案1所述，當前受支援的AnyConnect客戶端不再協商SSLv3，因此客戶端將無法連線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，對於使用v3.0.x和v3.1.x AnyConnect版本且已被棄用的部署(它們都是AnyConnect構建版本PRE 3.1.05182)，並且其中專門使用SSLv3協商，唯一的解決方案是不再使用SSLv3，或者考慮客戶端升級。

4. POODLE BITES的實際修補程式(思科錯誤ID CSCus08101)將僅整合到最新的臨時版本中。您可以升級到具有解決此問題的修補程式的ASA版本。Cisco Connection Online(CCO)上的第一個可用版本是9.3(2.2)版。

   針對此漏洞的第一批修復ASA軟體版本如下：
   8.2培訓： 8.2.5.558.4培訓： 8.4.7.269.0系列： 9.0.4.299.1系列： 9.1.69.2系列： 9.2.3.39.3培訓： 9.3.2.2

TLSv1.2

- 自軟體版本9.3(2)起，ASA支援TLSv1.2。
- AnyConnect版本4.x客戶端都支援TLSv1.2。

這意味著：

- 如果您使用無客戶端WebVPN，則任何運行該版本或更高版本的ASA都可以協商TLSv1.2。
- 如果使用AnyConnect客戶端，為了使用TLSv1.2，您需要升級到版本4.x客戶端。

相關資訊

- CVE-2014-8730
- 思科錯誤ID CSCug51375
- 思科錯誤ID CSCur42776
- 技術支援與文件 - Cisco Systems