SSL v3和TLS v1協定弱CBC模式漏洞

目錄

簡介

本檔案介紹如何在思科電子郵件安全裝置(ESA)上停用密碼塊連結(CBC)模式密碼。安全審計/掃描可能會報告ESA存在安全套接字層(SSL)v3/傳輸層安全(TLS)v1協定弱CBC模式漏洞。

> **注意**:如果運行的是較早的AsyncOS for Email Security代碼，建議升級到11.0.3版或更高版本。 有關最新版本和資訊，請參閱思科電子郵件安全發行說明。 如果您在升級或禁用密碼方面需要進一步協助，請開啟支援案例。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於AsyncOS for Email Security（任何版本）、Cisco ESA和虛擬ESA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

- 支付卡行業資料安全標準(PCI DSS)合規性要求禁用CBC密碼。
- 安全審計/掃描已識別出使用CBC模式密碼的SSL v3/TLS v1協定的潛在漏洞。

> **提示：**SSL版本3.0(RFC-6101)是過時和不安全的通訊協定。SSLv3 CVE-2014-3566中存在漏洞，該漏洞稱為Padding Oracle on Downgraded Legacy Encryption(POODLE)攻擊，思科錯誤ID CSCur27131。建議您在更改密碼並僅使用TLS時禁用SSL v3，並選擇選項3(TLS v1)。檢視提供的思科錯誤ID CSCur27131，瞭解完整的詳細資訊。

使用SSL v3和TLS v1協定是為了向其他協定(如HTTP和輕量級目錄訪問協定(LDAP))提供完整性、真實性和隱私性。 這些服務通過使用加密保護隱私、使用x509證書保護真實性，以及單向加密功能保護完整性。為了加密資料，SSL和TLS可以使用塊密碼，這些加密演算法僅可以將原始資料的固定塊加密到相同大小的加密塊。請注意，這些密碼將始終獲取相同原始資料塊相同的結果塊。為了獲得輸出的差異，加密的輸出與稱為初始化向量(IV)的具有相同大小的另一個塊進行XOR運算。CBC對初始塊使用一個IV，對後續的每個塊使用前一個塊的結果，以獲得塊密碼加密輸出的差值。

在SSL v3和TLS v1實現中，選擇CBC模式使用率很低，因為整個流量共用一個CBC會話與一組初始IV。如前所述，其餘的IV是先前塊加密的結果。隨後的靜脈注射可供竊聽者使用。這使得攻擊者能夠向純文字檔案流（由客戶端加密）中注入任意流量，以驗證其對注入塊之前的純文字檔案的猜測。如果攻擊者的猜測是正確的，則兩個資料塊的加密輸出是相同的。

對於低熵資料，可以用相對低的嘗試次數來猜測純文字檔案塊。例如，對於具有1000種可能性的資料，嘗試次數可以是500。

需求

要利用漏洞，必須滿足以下幾項要求：

1. SSL/TLS連線必須使用某個使用CBC模式的塊加密密碼，例如DES或AES。 使用RC4等流密碼的通道不受該漏洞的影響。大部分SSL/TLS連線使用RC4。
2. 只有擷取SSL/TLS連線上的資料，並且在該連線上主動傳送新資料的人才能利用此漏洞。漏洞的利用導致SSL/TLS連線終止。攻擊者必須繼續監控並使用新的連線，直到收集到足夠的資料來解密消息。
3. 由於每次都終止連線，因此SSL/TLS客戶端必須能夠繼續重新建立SSL/TLS通道足夠長的時間來解密消息。
4. 應用程式必須在它所建立的每個SSL/TLS連線上重新傳送相同的資料，監聽程式必須能夠在資料流中查詢它。IMAP/SSL等具有要登入的固定消息集的協定符合此要求。一般Web瀏覽則不會。

威脅

CBC漏洞是TLS v1的一個漏洞。此漏洞自2004年初以來一直存在，並在TLS v1.1和TLS v1.2的較新版本中已解決。

在用於郵件安全的AsyncOS 9.6之前，ESA使用TLS v1.0和CBC模式密碼。隨著AsyncOS 9.6的發佈，ESA引入了TLS v1.2。但可以禁用CBC模式密碼，並且只能使用不受該漏洞影響的RC4密碼。

此外，如果啟用SSLv2，可能會觸發此漏洞的誤報。禁用SSL v2非常重要。

解決方案

> **注意**:如果運行的是較早的AsyncOS for Email Security代碼，建議升級到11.0.3版或更高版本。 有關最新版本和資訊，請參閱思科電子郵件安全發行說明。 如果您在升級或禁用密碼方面需要進一步協助，請開啟支援案例。

禁用CBC模式密碼，以便僅啟用RC4密碼。將裝置設定為僅使用TLS v1或TLS v1/TLS v1.2:

1. 登入到CLI。
2. 輸入命令**sslconfig**。
3. 輸入命令**GUI**。
4. 為「TLS v1」選擇選項3，或如AsyncOS 9.6「TLS v1/TLS v1.2」中所列。
5. 輸入此密碼：
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. 輸入以下命令：**入站**。
7. 為「TLS v1」選擇選項3，或如AsyncOS 9.6「TLS v1/TLS v1.2」中所列。
8. 輸入此密碼：
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. 輸入命令**OUTBOUND**。
10. 為「TLS v1」選擇選項3，或如AsyncOS 9.6「TLS v1/TLS v1.2」中所列。
11. 輸入此密碼：
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. 按**Enter鍵**，直到返回主機名提示符。
13. 輸入命令**commit**。
14. 完成提交更改。

ESA現在配置為僅支援TLS v1或TLSv1/TLS v1.2（使用RC4密碼），同時禁止任何CBC過濾器。

以下是設定RC4:-SSLv2時使用的密碼清單。請注意，清單中沒有CBC模式密碼。

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

雖然這種漏洞因其複雜性和漏洞利用的要求而很少受到關注，但是這些步驟的執行對於防止可能的漏洞利用以及通過嚴格的安全掃描來說是一種很好的保障。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems