SSLv3和TLSv1协议弱CBC模式漏洞

目录

简介

本文描述如何禁用密码链块(CBC)在思科电子邮件安全工具(ESA)的模式密码器。安全跟踪/扫描也许报道ESA有安全套接字协议层(SSL) v3/Transport层安全(TLS) v1协议弱CBC模式漏洞。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据电子邮件安全(任何版本)，思科ESA和虚拟ESA的AsyncOS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

- 付款卡德行业数据安全标准的(PCI DSS)标准要求将禁用的CBC密码器。
- 安全跟踪/扫描识别与使用CBC模式密码器的SSL v3/TLS v1协议的潜在弱点。

提示：SSL版本3.0 (RFC-6101)是过时和不安全协议。有在叫作填充在Downgraded传统加密

(长卷毛狗)攻击的Oracle CVE-2014-3566的一个漏洞的SSLv3， Cisco Bug ID CSCur27131。建议是禁用SSL v3，当您更换密码器并且使用仅时TLS，并且选择选项3 (TLS v1)。查看提供的Cisco Bug ID CSCur27131关于完整详细信息。

SSL v3和TLS v1协议用于为了提供完整性、真实性和保密性给其他协议例如HTTP和轻量级目录访问协议(LDAP)。他们提供这些服务使用加密为保密性、x509证书为真实性和单程加密性能为完整性。为了加密数据， SSL和TLS能使用是加密算法能加密原始数据仅一已修复块到相同大小的一已加密块的分组加密。注意这些密码器永远将得到数据同一原始块的同一发生的块。为了达到差异在输出中，加密输出是XORed用指初始化矢量相同大小的另外块(iv)。CBC最初的块和上一个块的结果的用途一IV每随后的块的为了获取差异在分组加密加密中输出。

在SSL v3和TLS v1实施，因为整个流量共享有一套最初的IVs的，一CBC会话选择CBC模式使用情况差。IVs的其余是，如以前被提及，上一个块的加密的结果。随后的IVs供给窃听者。这允许一名攻击者以功能注入任意流量明文数据流(将由客户端加密)为了验证先于被注入的块的他们的明文猜测。如果攻击者猜测正确，则加密的输出是相同的为两块。

对于低熵数据，相对猜测明文块用尝试低数值是可能的。例如，为有1000种可能性的数据，尝试次数可以是500。

要求

有必须符合为了检测安全漏洞代码能工作的几个需求：

1. SSL/TLS连接必须使用使用CBC模式的其中一块加密密码器，例如DES或AES。 使用流密码例如RC4的信道不是受缺点支配。SSL/TLS连接的一个大比例使用RC4。
2. 漏洞可能由拦截在SSL/TLS连接的数据的人，并且发送在该连接的新建的数据积极只使用。缺点的开发造成SSL/TLS连接终止。攻击者必须继续监控和使用新连接，直到足够的数据收集解密消息。
3. 因为连接每次终止， SSL/TLS客户端一定能继续重建SSL/TLS信道太久能将解密的消息的。
4. 应用程序必须再发出在创建的每SSL/TLS连接的同一个数据，并且监听程序在数据流一定能找出它。协议类似有登陆固定的一组的消息满足此需求的IMAP/SSL。一般Web浏览不。

威胁

CBC漏洞是与TLS v1的一个漏洞。此漏洞是现有从早期2004年和被解决了在TLS v1.1和TLS v1.2最新版本。

在电子邮件安全的AsyncOS 9.6之前， ESA使用TLS v1.0和CBC模式密码器。使用版本AsyncOS 9.6， ESA介绍TLS v1.2。 但是， CBC模式密码器可以禁用，并且RC4仅的密码器不是受缺点支配可以使用。

另外，如果SSLv2启用这能触发此漏洞的一错误肯定。重要的是非常SSL v2禁用。

解决方案

禁用CBC模式密码器为了留给RC4仅密码器启用。设置设备只使用TLS v1或者TLS v1/TLS v1.2 ：

1. 登陆对CLI。
2. 输入命令**sslconfig**。
3. 输入命令**GUI**。
4. 选择如在AsyncOS 9.6"列出的选件编号3 “TLS的v1"，或者TLS v1/TLS v1.2"。
5. 输入此密码器：`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. 输入命令：**入站**。
7. 选择如在AsyncOS 9.6"列出的选件编号3 “TLS的v1"，或者TLS v1/TLS v1.2"。
8. 输入此密码器：`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. 输入outbound命令。
10. 选择如在AsyncOS 9.6"列出的选件编号3 “TLS的v1"，或者TLS v1/TLS v1.2"。
11. 输入此密码器：`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. 请按回车，直到您回到主机名提示符。
13. 输入commit命令。
14. 确认您的更改的Finalize。

当禁止所有CBC过滤器时， ESA当前配置只支持TLS v1或者TLSv1/TLS v1.2，用RC4密码器。

这是使用的密码器列表，当您集RC4:-SSLv2。注意没有在列表的CBC模式密码器。

```
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
```

当此检测安全漏洞代码是非常低重要的事物由于其复杂性和需求使用时，这些步骤性能是可能的检测安全漏洞代码的预防的一个巨大保障，以及通过严格安全扫瞄。

相关信息

- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems