禁用SSH服务器CBC在ASA的模式密码器

目录

简介

本文描述如何禁用SSH服务器CBC在ASA的模式密码器。在扫描漏洞CVE-2008-5161描述使用在密码链块(CBC)模式的一种分组加密算法，在SSH会话上使容易为了远端攻击者能恢复某些纯文本数据从密码文本一任意块通过未知向量。

密码链块(CBC)是密码器块的操作模式，此算法使用分组加密提供一信息性服务例如机密性或真实性。

先决条件

要求

Cisco 建议您了解以下主题：

- 可适应安全工具ASA平台体系结构
- 密码链块(CBC)

使用的组件

本文档中的信息根据与OS 9.6.1的思科ASA 5506。

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。如果您的网络实际，请保证您了解所有命令潜在影响。

问题

默认情况下，在ASA CBC模式在可能是用户信息的一个漏洞的ASA启用。

解决方案

在增强CSCum63371以后，能力修改ASA SSH密码器在版本9.1(7)介绍，但是正式有ssh命令**密码器加密**和**SSH密码器完整性的**版本是9.6.1。

为了禁用CBC在SSH的模式密码器请遵从此步骤：

运行“sh run所有SSH”在ASA ：

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

如果看到ssh命令**密码器加密介质**默认情况下在ASA设置的这意味着ASA使用中等和高强度密码器。

为了看到在ASA的可用的SSH加密算法，请运行show ssh命令**密码器**：

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
       all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr
aes256-ctr
       fips:    aes128-cbc   aes256-cbc
       high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
       all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
       medium:  hmac-sha1    hmac-sha1-96
       fips:    hmac-sha1
       high:    hmac-sha1
```

输出显示所有可用的加密算法： **3DES CBC aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。**

为了禁用CBC模式，因此它在SSH配置可以使用，定制加密算法，与以下命令一起使用：

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

在这执行后，请运行show run命令**所有SSH**，当前在SSH密码器加密配置里仅所有算法使用CTR模式：

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

同样， SSH完整性算法可以修改以ssh命令**密码器完整性。**