在 ASA 上禁用 SSH 服务器 CBC 模式密码

目录

简介

本文档说明了如何在 ASA 上禁用 SSH 服务器 CBC 模式密码器。关于扫描漏洞 CVE-2008-5161 的记录说明，在密码块链接 (CBC) 模式下使用分组密码算法，使得远程攻击者更容易通过未知攻击途径从 SSH 会话中的任意区块密码文本恢复某些纯文本数据。

密码块链接 (CBC) 是密码块的一种操作模式，此算法使用分组密码来提供信息服务，例如保密性或真实性。

先决条件

要求

Cisco 建议您了解以下主题：

- 自适应安全设备 ASA 平台架构
- 密码块链接 (CBC)

使用的组件

本文档的信息基于 Cisco ASA 5506（操作系统版本为 9.6.1）。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

ASA 会默认启用 CBC 模式，这可能成为客户信息的漏洞。

解决方案

在 CSCum63371 带来增强功能之后，版本 9.1(7) 引入修改 ASA SSH 密码的功能，但版本 9.6.1 才正式支持命令 ssh cipher encryption 和 sssh cipher integrity。

要在 SSH 上禁用 CBC 模式密码，请执行以下程序：

在 ASA 上运行“sh run all ssh”：

```
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
```

如果输出显示 ssh cipher encryption medium，这意味着 ASA 的默认设置是使用中高强度密码。

要查看 ASA 中可用的 ssh 加密算法，运行命令 show ssh ciphers：

```
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-c
        low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        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。

要禁用 CBC 模式而让其在 ssh 配置上可用，请运行以下命令来自定义要采用的加密算法：

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

完成此操作后，运行命令 show run all ssh，结果就是在 ssh 密码加密配置中，所有算法仅使用 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，可以使用 ssh cipher integrity 命令来修改 SSH 完整性算法。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。