排除NCCM 3.8+和CSPC 2.9+中的CBC密码漏洞

目录

简介

本文档介绍如何对NCCM 3.8+和CSPC 2.9+中的CBC密码漏洞进行故障排除。

问题

在CSPC/NCCM的最新版本中，我们存在CBC弱密码漏洞。在大多数情况下，可以通过更新所需的ssh配置文件来修复此问题。但是，本文提出明确拒绝他们通过加密策略进行访问。如果其他方法都失败，请使用此方法。这不会影响默认加密策略，而是在默认策略之上添加额外的层。

传统方法

确保已从sshd_config中删除所有CVC密码。如果问题仍然存在，您可以在/etc/sysconfig/sshd下为参数提供空白条目。

```
CRYPTO_POLICY=
```

在进行任何修改之前，请确保进行备份。

要验证此操作是否有效，请在远程计算机上运行此命令：

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

如果系统提示您输入密码或添加RSA密钥，则问题仍然存在。

解决方案

如果上述过程失败，您可以通过明确拒绝对CBC密码的任何访问来添加额外的加密策略层。我们不建议更改任何加密策略默认配置，因此建议使用此方法。

在继续之前，请确保在默认加密策略的上方没有应用其他层。如果有附加层，则可以在进行任何更改之前查看这些层。要检查这一点，请运行以下命令：

```
update-crypto-policies --show
```

响应为DEFAULT。如果是，则无需任何进一步验证即可继续执行后续步骤。

在绝对路径下创建新文件：

```
/etc/crypto-policies/policies/modules/DISABLE-CBC.pmod
```

您可以以任何方式命名此文件，但扩展名以.pmod结尾。

由于我们将删除此漏洞以使用这些密码限制ssh访问，请将此行输入为此新文件中的唯一条目：

```
ssh_cipher = -AES-128-CBC -AES-256-CBC
```

注意：此乃仅供参考。您可以添加您明确尝试拒绝的所有密码，但建议您为除CBC外的任何密码创建一个新文件，以避免混淆。

保存文件后，通过运行以下命令，将加密策略的值从DEFAULT设置到此附加层：

```
update-crypto-policies --set DEFAULT:DISABLE-CBC
```

同样，DISABLE-CBC值可能因创建文件时提供的名称而异。

现在可以通过运行以下命令重新检查：

```
update-crypto-policies --show
```

这次，它显示DEFAULT:DISABLE-CBC，确认已添加了一个附加层，但未修改默认文件。

在此阶段，如果重新验证访问，则会拒绝访问：

```
ssh -vv -oCiphers=aes128-cbc,aes256-cbc 127.0.0.1
```

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）。