Solucionar problemas de vulnerabilidade de cifra CBC no NCCM 3.8+ e CSPC 2.9+

Contents

Introdução

Este documento descreve como solucionar problemas de vulnerabilidade de cifra CBC no NCCM 3.8+ e no CSPC 2.9+.

Problema

Nas versões recentes do CSPC/NCCM, temos uma vulnerabilidade de cifra fraca do CBC. Na maioria dos casos, você poderia corrigi-lo atualizando os arquivos de configuração ssh desejados. No entanto, este artigo foi levantado para negar explicitamente seu acesso através de políticas de criptografia. Use isto se tudo falhar. Isso não pode afetar as políticas de criptografia padrão, mas adicionar uma camada adicional sobre a política padrão.

Abordagem tradicional

Verifique se todas as cifras CVC foram removidas de sshd_config. Se o problema ainda persistir, você pode fornecer uma entrada em branco para o parâmetro em /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

Certifique-se de fazer um backup antes de fazer qualquer modificação.

Para verificar se isso funcionou, execute este comando em sua máquina remota:

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

Se for solicitada uma senha ou se forem adicionadas chaves RSA, o problema ainda persiste.

Solução

Se o procedimento anterior falhar, você poderá adicionar uma camada adicional de política de criptografia negando explicitamente qualquer acesso às cifras CBC. Não recomendamos alterar nenhuma configuração padrão de política de criptografia, portanto, essa abordagem é recomendada.

Antes de prosseguir, verifique se não há camadas adicionais aplicadas sobre a política de criptografia DEFAULT. Se houver camadas adicionais, você poderá revisá-las antes de fazer qualquer alteração. Para verificar isso, execute este comando:

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

A resposta é DEFAULT. Se estiver, você poderá prosseguir com as próximas etapas sem qualquer verificação adicional.

Crie um novo arquivo no caminho absoluto:

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

Você pode nomear esse arquivo de qualquer maneira, mas a extensão termina em .pmod.

Como estamos removendo essa vulnerabilidade para restringir o acesso ao ssh usando essas cifras, insira esta linha como a única entrada neste novo arquivo:

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

Note: Isto é apenas para referência. Você pode adicionar todas as cifras que está tentando negar explicitamente, mas é aconselhável criar um novo arquivo para qualquer cifra diferente de CBC para evitar confusão.

Depois de salvar o arquivo, defina o valor das políticas de criptografia de DEFAULT para esta camada adicional executando este comando:

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

Novamente, o valor DISABLE-CBC pode ser diferente com base no nome fornecido quando você criou o arquivo.

Agora você pode verificar novamente executando:

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

Desta vez, ele mostra DEFAULT:DISABLE-CBC, confirmando que uma camada adicional foi adicionada sem modificar o arquivo padrão.

Neste estágio, se você verificar novamente o acesso, ele será negado:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.