# Problemen met CBC-coderingskwetsbaarheid in NCCM 3.8+ en CSPC 2.9+ oplossen

## Inhoud



## Inleiding

In dit document wordt beschreven hoe problemen met CBC-coderingslekken in NCCM 3.8+ en CSPC 2.9+ kunnen worden opgelost.

## Probleem

In de recente releases van CSPC / NCCM hebben we een CBC-zwakke cijferkwetsbaarheid. In de meeste gevallen kunt u het oplossen door de gewenste ssh-configuratiebestanden bij te werken. Dit artikel is echter aangehaald om hun toegang expliciet te weigeren via crypto-beleid. Gebruik dit als al het andere faalt. Dit kan geen invloed hebben op het standaard crypto-beleid, maar eerder een extra laag bovenop het standaardbeleid toevoegen.

### traditionele aanpak

Controleer of alle CVC-coderingen uit sshd_config zijn verwijderd. Als het probleem zich blijft voordoen, kunt u een leeg item opgeven voor de parameter onder /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

Zorg ervoor dat u een back-up maakt voordat u wijzigingen aanbrengt.

Voer deze opdracht uit op het externe systeem om te controleren of dit werkt:

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

Als u wordt gevraagd om een wachtwoord of het toevoegen van RSA-sleutels, dan blijft het probleem bestaan.

# Oplossing

Als de vorige procedure mislukt, kunt u een extra laag crypto-beleid toevoegen door expliciet de toegang tot CBC-coderingen te weigeren. We raden niet aan om de standaardconfiguratie van het cryptobeleid te wijzigen, dus deze aanpak wordt geadviseerd.

Voordat we verder gaan, moet u ervoor zorgen dat er geen extra lagen worden aangebracht bovenop het standaard crypto-beleid. Als er extra lagen zijn, kunt u deze bekijken voordat u wijzigingen aanbrengt. Voer deze opdracht uit om dit te controleren:

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

Het antwoord is standaard. Als dit het geval is, kunt u doorgaan met de volgende stappen zonder verdere verificatie.

Maak een nieuw bestand onder het absolute pad:

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

U kunt dit bestand op elke manier een naam geven, maar de extensie eindigt op .pmod.

Aangezien we deze kwetsbaarheid verwijderen om de toegang tot ssh te beperken met behulp van deze cijfers, voert u deze regel in als de enige vermelding in dit nieuwe bestand:

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

---

Opmerking: dit is alleen ter referentie. U kunt alle cijfers toevoegen die u expliciet probeert te ontkennen, maar het wordt geadviseerd om een nieuw bestand te maken voor een ander cijfer dan CBC om verwarring te voorkomen.

---

Nadat u het bestand hebt opgeslagen, stelt u de waarde van het cryptobeleid van STANDAARD in op deze extra laag door deze opdracht uit te voeren:

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

Nogmaals, de waarde DISABLE-CBC kan verschillen op basis van de naam die is opgegeven toen u het bestand hebt gemaakt.

U kunt het nu opnieuw controleren door uit te voeren:

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

Deze keer wordt DEFAULT:DISABLE-CBC weergegeven, waarmee wordt bevestigd dat een extra laag is toegevoegd zonder het standaardbestand te wijzigen.

In dit stadium, als u de toegang opnieuw verifieert, wordt deze geweigerd:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.