Fehlerbehebung bei CBC Cipher-Schwachstellen in NCCM 3.8+ und CSPC 2.9+

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der CBC Cipher-Schwachstelle in NCCM 3.8+ und CSPC 2.9+ beschrieben.

Problem

In den letzten Versionen von CSPC/NCCM besteht eine Schwachstelle hinsichtlich CBC-Verschlüsselung. In den meisten Fällen können Sie das Problem beheben, indem Sie die gewünschten SSH-Konfigurationsdateien aktualisieren. In diesem Artikel wird jedoch ausdrücklich darauf hingewiesen, dass der Zugriff durch Krypto-Richtlinien verweigert wird. Verwenden Sie diese Option, wenn alles andere fehlschlägt. Dies kann sich nicht auf die Standard-Kryptografierichtlinien auswirken, sondern fügt der Standardrichtlinie eine zusätzliche Ebene hinzu.

Traditioneller Ansatz

Stellen Sie sicher, dass alle CVC-Chiffren aus "sshd_config" entfernt wurden. Wenn das Problem weiterhin besteht, können Sie unter /etc/sysconfig/sshd einen leeren Eintrag für den Parameter angeben.

```
CRYPTO_POLICY=
```

Stellen Sie sicher, dass Sie eine Sicherung durchführen, bevor Sie Änderungen vornehmen.

Führen Sie den folgenden Befehl auf dem Remotecomputer aus, um zu überprüfen, ob dies funktioniert hat:

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

Wenn Sie zur Eingabe eines Kennworts oder zum Hinzufügen von RSA-Schlüsseln aufgefordert werden, besteht das Problem weiterhin.

Lösung

Wenn das vorherige Verfahren fehlschlägt, können Sie eine zusätzliche Ebene der Kryptografierichtlinie hinzufügen, indem Sie den Zugriff auf CBC-Verschlüsselungen explizit verweigern. Es wird nicht empfohlen, die Standardkonfiguration der Krypto-Richtlinie zu ändern. Daher wird dieser Ansatz empfohlen.

Bevor wir fortfahren, stellen Sie sicher, dass keine zusätzlichen Ebenen auf die STANDARD-Kryptografierichtlinie angewendet werden. Wenn zusätzliche Ebenen vorhanden sind, können Sie diese überprüfen, bevor Sie Änderungen vornehmen. Führen Sie den folgenden Befehl aus, um dies zu überprüfen:

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

Die Antwort lautet STANDARD. Ist dies der Fall, können Sie ohne weitere Überprüfung mit den nächsten Schritten fortfahren.

Erstellen Sie eine neue Datei unter dem absoluten Pfad:

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

Sie können diese Datei beliebig benennen, aber die Erweiterung endet in .pmod.

Da wir diese Verwundbarkeit beseitigen, um den Zugriff auf SSH mit diesen Chiffren zu beschränken, geben Sie diese Zeile als einzigen Eintrag in diese neue Datei ein:

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

Anmerkung: Dies dient nur zu Referenzzwecken. Sie können alle Chiffren hinzufügen, die Sie explizit zu verweigern versuchen, aber es wird empfohlen, eine neue Datei für jede andere Chiffre als CBC zu erstellen, um Verwirrung zu vermeiden.

Legen Sie nach dem Speichern der Datei den Wert der Kryptografierichtlinien von STANDARD auf diese zusätzliche Ebene fest, indem Sie den folgenden Befehl ausführen:

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

Auch hier kann sich der Wert DISABLE-CBC je nach dem Namen unterscheiden, der beim Erstellen der Datei angegeben wurde.

Jetzt können Sie die Überprüfung erneut durchführen, indem Sie:

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

Dieses Mal wird DEFAULT:DISABLE-CBC angezeigt und bestätigt, dass eine zusätzliche Ebene hinzugefügt wurde, ohne die Standarddatei zu ändern.

Wenn Sie den Zugriff erneut überprüfen, wird Folgendes verweigert:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.