NCCM 3.8+ 및 CSPC 2.9+에서 CBC 암호화 취약성 문제 해결

목차

소개

이 문서에서는 NCCM 3.8+ 및 CSPC 2.9+에서 CBC 암호 취약성을 트러블슈팅하는 방법을 설명합니다.

문제

최근 릴리스된 CSPC/NCCM에서는 CBC 약한 암호화 취약성이 있습니다. 대부분의 경우 원하는 ssh 컨피그레이션 파일을 업데이트하여 수정할 수 있습니다. 그러나 이 글은 암호화 정책을 통해 명시적으로 액세스를 거부하기 위해 제기된 것이다. 다른 모든 것이 실패하는 경우 이 옵션을 사용합니다. 이는 기본 암호화 정책에 영향을 줄 수 없으며, 오히려 기본 정책 위에 추가 레이어를 추가합니다.

기존 방식

모든 CVC 암호가 sshd_config에서 제거되었는지 확인합니다. 문제가 지속되면 /etc/sysconfig/sshd 아래의 매개변수에 빈 항목을 제공할 수 있습니다.

```
CRYPTO_POLICY=
```

수정하기 전에 백업을 수행해야 합니다.

이 명령이 실행되었는지 확인하려면 원격 시스템에서 다음 명령을 실행합니다.

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

비밀번호를 입력하라는 메시지가 표시되거나 RSA 키를 추가하는 경우 문제가 계속 발생합니다.

솔루션

이전 절차가 실패하면 CBC 암호에 대한 액세스를 명시적으로 거부하여 암호화 정책의 추가 레이어를 추가할 수 있습니다. 암호화 정책 기본 컨피그레이션은 변경하지 않는 것이 좋습니다. 따라서 이 방법을 사용하는 것이 좋습니다.

계속 진행하기 전에 기본 암호화 정책 위에 추가 레이어가 적용되지 않았는지 확인합니다. 추가 레이어가 있는 경우 변경하기 전에 레이어를 검토할 수 있습니다. 이를 확인하려면 다음 명령을 실행합니다.

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

응답은 DEFAULT입니다. 그렇다면 추가 확인 없이 다음 단계를 진행할 수 있습니다.

절대 경로 아래에 새 파일을 만듭니다.

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

확장명이 .pmod로 끝나지만 어떤 방법으로든 이 파일의 이름을 지정할 수 있습니다.

이러한 암호를 사용하여 ssh 액세스를 제한하기 위해 이 취약성을 제거하고 있으므로 이 새 파일에 이 행만 입력합니다.

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

참고: 이는 참조용입니다. 명시적으로 거부하려는 모든 암호를 추가할 수 있지만, 혼동을 피하려면 CBC 이외의 암호에 대해 새 파일을 생성하는 것이 좋습니다.

파일을 저장한 후 다음 명령을 실행하여 crypto-policies의 값을 DEFAULT에서 이 추가 레이어로 설정합니다.

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

다시, DISABLE-CBC 값은 파일을 만들 때 제공된 이름에 따라 다를 수 있습니다.

이제 다음을 실행하여 다시 확인할 수 있습니다.

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

이번에는 DEFAULT:DISABLE-CBC를 표시하여 기본 파일을 수정하지 않고 추가 레이어를 추가했음을 확인합니다.

이 단계에서 액세스를 재검증하면 액세스가 거부됩니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.