Resolución de problemas de vulnerabilidad de cifrado CBC en NCCM 3.8+ y CSPC 2.9+

Contenido

Introducción

Este documento describe cómo resolver problemas de vulnerabilidad de cifrado CBC en NCCM 3.8+ y CSPC 2.9+.

Problema

En las últimas versiones de CSPC/NCCM, tenemos una vulnerabilidad de cifrado CBC débil. En la mayoría de los casos, puede arreglarlo actualizando los archivos de configuración ssh deseados. Sin embargo, este artículo se ha planteado para denegar explícitamente su acceso a través de políticas criptográficas. Use esto si todo lo demás falla. Esto no puede afectar a las políticas de cifrado predeterminadas, sino que más bien agrega una capa adicional sobre la política predeterminada.

Enfoque tradicional

Asegúrese de que todos los cifrados CVC se hayan eliminado de sshd_config. Si el problema persiste, puede proporcionar una entrada en blanco al parámetro en /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

Asegúrese de realizar una copia de seguridad antes de realizar cualquier modificación.

Para verificar si esto ha funcionado, ejecute este comando en su máquina remota:

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

Si se le solicita una contraseña o que agregue claves RSA, el problema continúa.

Solución

Si el procedimiento anterior falla, puede agregar una capa adicional de política criptográfica negando explícitamente cualquier acceso a los cifrados CBC. No se recomienda cambiar ninguna configuración predeterminada de la política de cifrado, por lo que se recomienda este enfoque.

Antes de continuar, asegúrese de que no haya capas adicionales aplicadas sobre la política criptográfica PREDETERMINADA. Si hay capas adicionales, puede revisarlas antes de realizar cambios. Para comprobarlo, ejecute este comando:

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

La respuesta es DEFAULT. Si es así, puede continuar con los siguientes pasos sin ninguna otra verificación.

Cree un nuevo archivo en la ruta absoluta:

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

Puede asignar un nombre a este archivo de cualquier manera, pero la extensión termina en .pmod.

Debido a que estamos eliminando esta vulnerabilidad para restringir el acceso a ssh usando estos cifrados, ingrese esta línea como la única entrada en este nuevo archivo:

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

Nota: Esto es sólo para referencia. Puede agregar todos los cifrados que esté intentando denegar explícitamente, pero se recomienda crear un nuevo archivo para cualquier cifrado que no sea CBC para evitar confusiones.

Después de guardar el archivo, establezca el valor de las políticas crypto de DEFAULT en esta capa adicional ejecutando este comando:

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

Una vez más, el valor DISABLE-CBC puede diferir en función del nombre proporcionado al crear el archivo.

Ahora puede volver a realizar la comprobación ejecutando:

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

Esta vez, muestra DEFAULT:DISABLE-CBC, confirmando que se ha agregado una capa adicional sin modificar el archivo predeterminado.

En esta etapa, si vuelve a verificar el acceso, se le deniega:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).