Risoluzione dei problemi relativi alla vulnerabilità della crittografia CBC in NCCM 3.8+ e CSPC 2.9+

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alla vulnerabilità della crittografia CBC in NCM 3.8+ e CSPC 2.9+.

Problema

Nelle recenti release di CSPC/NCCM, abbiamo una vulnerabilità di cifratura debole CBC. Nella maggior parte dei casi, è possibile risolvere il problema aggiornando i file di configurazione ssh desiderati. Tuttavia, questo articolo è stato sollevato per negare esplicitamente il loro accesso attraverso le policy di crittografia. Utilizzatelo se tutto il resto fallisce. Ciò non può influire sui criteri di crittografia predefiniti, ma è preferibile aggiungere un livello aggiuntivo al criterio predefinito.

Approccio tradizionale

Accertarsi che tutte le cifrature CVC siano state rimosse da sshd_config. Se il problema persiste, è possibile fornire una voce vuota per il parametro in /etc/sysconfig/sshd.

```
CRYPTO_POLICY=
```

Assicurarsi di eseguire un backup prima di apportare qualsiasi modifica.

Per verificare il corretto funzionamento di questa operazione, eseguire questo comando sul computer remoto:

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

Se viene richiesta una password o vengono aggiunte chiavi RSA, il problema persiste.

Soluzione

Se la procedura precedente ha esito negativo, è possibile aggiungere un ulteriore livello di criteri di crittografia negando esplicitamente l'accesso alle cifrature CBC. Si sconsiglia di modificare la configurazione predefinita dei criteri di crittografia, pertanto si consiglia di utilizzare questo approccio.

Prima di procedere, verificare che non vi siano altri livelli applicati al criterio di crittografia PREDEFINITO. Se sono presenti livelli aggiuntivi, è possibile esaminarli prima di apportare qualsiasi modifica. Per verificare questa condizione, eseguire questo comando:

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

La risposta è DEFAULT. In caso affermativo, è possibile procedere con i passaggi successivi senza ulteriori verifiche.

Creare un nuovo file nel percorso assoluto:

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

È possibile denominare questo file in qualsiasi modo, ma l'estensione termina in .pmod.

Poiché si sta eliminando questa vulnerabilità per limitare l'accesso ssh utilizzando questi cifrari, immettere questa riga come unica voce in questo nuovo file:

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

Nota: Questo è solo a scopo di riferimento. È possibile aggiungere tutti i cifrari che si sta esplicitamente tentando di negare, ma si consiglia di creare un nuovo file per qualsiasi cifratura diversa da CBC per evitare confusione.

Dopo aver salvato il file, impostare il valore dei criteri di crittografia da DEFAULT a questo livello aggiuntivo eseguendo questo comando:

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

Anche in questo caso, il valore DISABLE-CBC può variare in base al nome fornito al momento della creazione del file.

È ora possibile ricontrollare eseguendo:

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

Questa volta, viene visualizzato DEFAULT:DISABLE-CBC, per confermare che è stato aggiunto un livello aggiuntivo senza modificare il file predefinito.

In questa fase, se si verifica nuovamente l'accesso, questo viene rifiutato:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).