Troubleshoot CBC Cipher Vulnerability in NCCM 3.8+ and CSPC 2.9+

Contents

Introduction

This document describes how to troubleshoot CBC Cipher Vulnerability in NCCM 3.8+ and CSPC 2.9+.

Problem

In the recent releases of CSPC/NCCM, we have a CBC weak cipher vulnerability. In most instances, you could fix it by updating the desired ssh config files. However, this article has been raised to explicitly deny their access through crypto policies. Use this if everything else fails. This cannot affect the default crypto policies but rather add an additional layer on top of the default policy.

Traditional Approach

Ensure all CVC ciphers have been removed from sshd_config. If the issue still persists, you can provide a blank entry to the parameter under **/etc/sysconfig/sshd**.

```
CRYPTO_POLICY=
```

Make sure to take a backup before doing any modification.

To verify if this has worked, run this command on your remote machine:

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

If you are prompted for a password or adding RSA keys, then the issue still persists.

Solution

If the previous procedure fails, you can add an additional layer of crypto policy by explicitly denying any access to CBC ciphers. We do not recommend changing any crypto policy default configuration, so this approach is advised.

Before we proceed, ensure there are no additional layers applied on top of the DEFAULT crypto polic. If there are additional layers, then you can review them before making any changes. To check this, run this command:

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

The response is **DEFAULT**. If it is, you can proceed with the next steps without any further verification.

Create a new file under the absolute path:

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

You can name this file in any manner but the extension ends in **.pmod**.

Since we are removing this vulnerability to restrict ssh access using these ciphers, enter this line as the only entry in this new file:

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

Note: This is for reference only. You can add all the ciphers that you are explicitly trying to deny, but it is advised to create a new file for any cipher other than CBC to avoid confusion.

After saving the file, set the value of crypto-policies from **DEFAULT** to this additional layer by running this command:

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

Again, **DISABLE-CBC** value can differ based on the name provided when you created the file.

You can now recheck by running:

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

This time, it shows **DEFAULT:DISABLE-CBC**, confirming that an additional layer has been added without modifying the default file.

At this stage, if you reverify the access, it is denied:

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