# FIX VA-kube

## api-server 6443

1. Find issues

```
nmap --script ssl-enum-ciphers -p 6443 127.0.0.1
```

output:

```
root@node2:~# nmap --script ssl-enum-ciphers -p 6443 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-21 14:09 +07
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).

PORT     STATE SERVICE
6443/tcp open  sun-sr-https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
```

> Got a warning.

2. Config kube-apiserver.yaml

```
vi /etc/kubernetes/manifests/kube-apiserver.yaml
```

add this line.

```
- --tls-cipher-
suites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_
SHA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_
WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_GCM_SHA384
```

3. Test

```
root@node2:~# nmap --script ssl-enum-ciphers -p 6443 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-21 14:12 +07
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).

PORT     STATE SERVICE
6443/tcp open  sun-sr-https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

## Etcd: (2379)

1. Find issues

```
nmap --script ssl-enum-ciphers -p 2379 127.0.0.1
```

output:

```
root@node3:~# nmap --script ssl-enum-ciphers -p 2379 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-21 14:35 +07
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).

PORT     STATE SERVICE
2379/tcp open  etcd-client
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
```

```
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Forward Secrecy not supported by any cipher
|_  least strength: C

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

2. Fix

```
vi /etc/kubernetes/manifests/etcd.yaml
```

add this line

```
- --cipher-
suites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_
SHA384
```

3. Test

```
nmap --script ssl-enum-ciphers -p 2379 127.0.0.1
```

output:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-09-11 18:44 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).

PORT     STATE SERVICE
2379/tcp open  etcd-client
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
```

```
|_  least strength: A

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

## Kubelet: (10250)

2. Fix