OpenVPN Sweet32 Vulnerability Remediation Steps (Disabling 3DES cipher suite)

Steps:

1.Login to Openvpn server using openvpnas username

2. Switch to root

3. Go to /usr/local/openvpn\_as/scripts

4. Exceute below :

* **./sacli ConfigQuery | grep -i "cs.openssl\_ciphersuites"**
* If nothing is returned that means default cipher suite is enabled which shows vulnerability
* To disable 3DES execute

**./sacli --key "cs.openssl\_ciphersuites" --value 'DEFAULT:!EXP:!PSK:!SRP:!LOW:!RC4:!3DES' ConfigPut**

**./sacli start**

you will get the below type result as new profile applied

RunStart warm None

{

"active\_profile": "Default",

"errors": {},

"service\_status": {

"api": "on",

"auth": "on",

"bridge": "on",

"client\_query": "on",

"crl": "on",

"daemon\_pre": "on",

"db\_push": "on",

"ip6tables\_live": "on",

"ip6tables\_openvpn": "on",

"iptables\_live": "on",

"iptables\_openvpn": "on",

"iptables\_web": "restarted",

"license": "on",

"log": "on",

"openvpn\_0": "on",

"user": "on",

"web": "restarted"

}

}

* then again check the cipher suite by executing the below:

**./sacli ConfigQuery | grep -i "cs.openssl\_ciphersuites"**

Result : "cs.openssl\_ciphersuites": "DEFAULT:!EXP:!PSK:!SRP:!LOW:!RC4:!3DES",

Now you can see 3DES diabled (!3DES)