某局点SecPath M9000(V7)防火墙漏洞修复不生效的经验案例

漏洞相关 丁佳欣 2021-07-24 发表

组网及说明

null

问题描述

现场反馈两台相同版本的M9006防火墙使用相同方法修复(CVE-2015-2808) SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞，但是其中一台修复后扫描漏洞仍然存在，修复失败，对此提出疑问。

过程分析

确认现场的漏洞修复方法无误，对比查看两台防火墙设备的配置发现修复失败的设备比成功修复的设备多配置了netconf功能，后续继续确认如果设备开启了netconf功能，那么需要在配置netconf功能时同样调用整改后的SSL 策略并且重启netconf服务，才能完全将存在漏洞的算法完全排除，或者删除netconf配置后也能够解决此问题。

解决方法

设备开启了netconf功能，在使用netconf功能时调用SSL 策略，并且重启netconf服务。

```
netconf over soap ssl server-policy test

ssl server-policy test
pki-domain test
ciphersuite rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha rsa_aes_128_cbc_sha256 rsa_aes_256_c
bc_sha256
#
netconf soap http enable
netconf soap https enable
```