

知 SSL证书链包含少于2048位的RSA密钥

PKI

SSL

漏洞相关

孔凡安

2022-03-14 发表

组网及说明

不涉及

问题描述

SSL证书链包含小于2048位的RSA密钥

此服务使用的X.509证书链包含小于2048位的RSA密钥的证书。

描述：远程主机发送的X.509证书中至少有一个密钥小于2048位。根据认证机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。在2014年1月1日之后，一些浏览器的SSL实现可能会拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销少于2048位的证书。注意，如果RSA密钥在2010年12月31日之前发布，那么Nessus不会将其标记为小于2048位的根证书，因为标准认为它们是豁免的。

过程分析

防火墙新版本的自签名证书密钥为2048位，可以将内置的证书导出并导入到扫描出该漏洞的老版本设备上。

可参考：<https://zhiliao.h3c.com/theme/details/164196>，<https://zhiliao.h3c.com/Theme/details/43650>

注：仅限于Comware V7的防火墙，导出前确认下该证书是否是2048位。

显示(S): <所有>

字段	值
签名哈希算法	sha256
颁发者	HTTPS-Self-Sign...
有效期从	2021年6月11日 1...
到	2041年6月6日 16...
使用者	HTTPS-Self-Sign...
公钥	RSA (2048 Bits)
公钥参数	05 00
基本约束	Subject Type=En...
指纹	0e45c2e7b2b5ef...

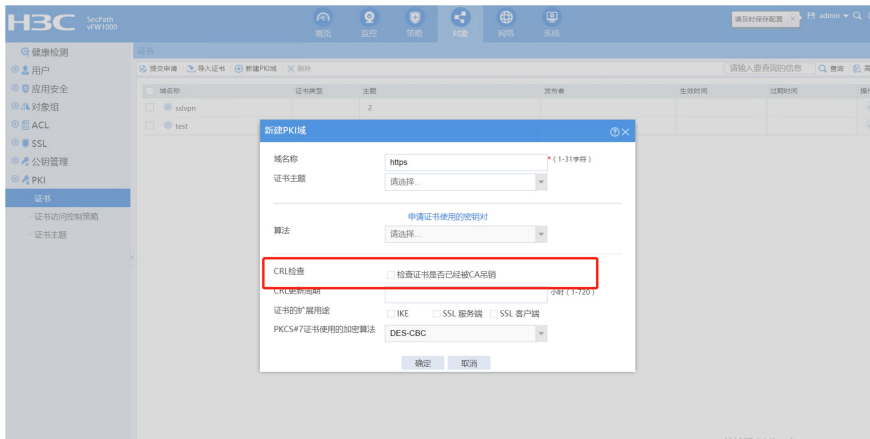

```
30 82 01 0a 02 82 01 01 00 c6 a2 ef 54 74 27 c9 49 7f 68 45 f9 6b 0e 7e
13 ea eb 6a 2c 27 35 e2 bb 87 1c d0 de 0b b9 b4 a1 88 66 43 cd cf 69 9f
51 91 c2 f7 99 5e 90 90 d6 d2 de 26 99 bf 5b f9 65 1c 52 cd dd ad 11 dd
77 fe 32 46 ac 11 67 33 84 a7 aa a4 b4 9f 72 fb 39 f7 df 61 b6 ad ce 6b
5d a8 a8 7d a9 f1 1c be 57 c2 26 7a 3e 28 45 ba 78 4c fb 07 7a 9d ee c2
6e 02 9e 10 9f 38 fe 16 d4 f9 d4 06 06 bd 8f af 91 5c a0 8d 3e 16 3a 5b
56 d1 92 2c 2f de 0b ef d9 82 c4 67 8d 8c 86 2a 77 7a f6 3b 99 48 4e 27
05 a8 13 72 5e e3 33 3a 46 f8 b6 c6 68 df a6 8d 1b ba d9 d2 70 29 b5 a1
71 6e bd 4f 9a fd 62 d5 0f a1 73 0f 6f e5 5c 2f 95 c7 d4 82 f2 95 58 d5 2c
```

编辑属性(E)... 复制到文件(C)...

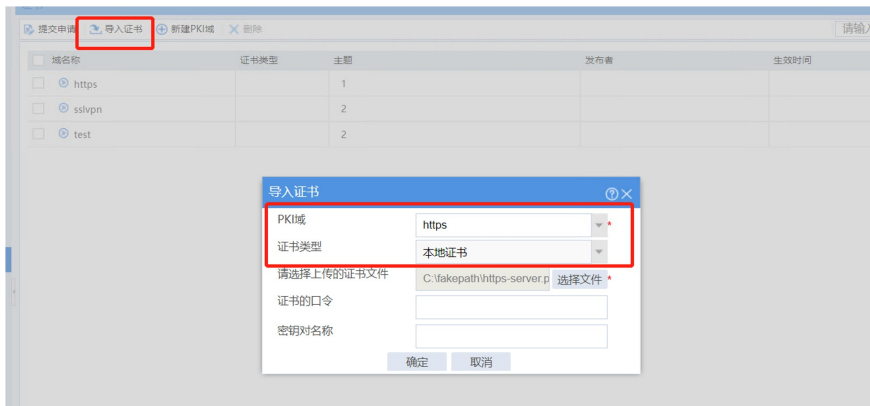
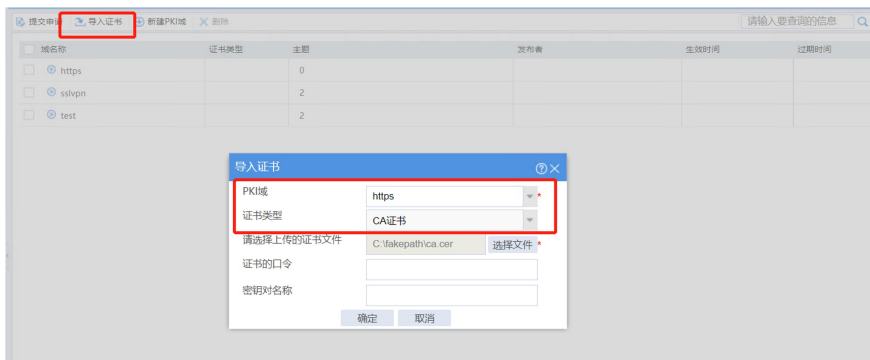
解决方法

步骤:

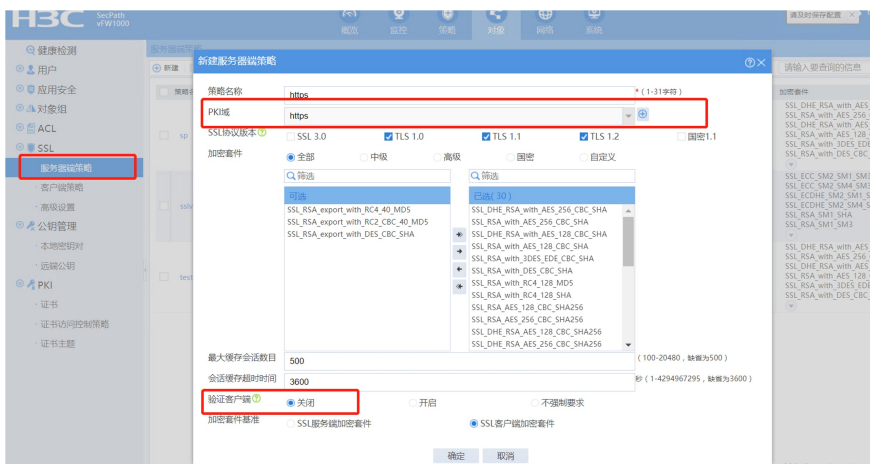
1.新建PKI域, 命名为https, "检查证书是否被CA吊销"取消勾选



2. 向pki域"https"分别导入CA证书, 和本地证书



3. 创建ssl服务器端策略, "https"并引用创建好的PKI域"https", 同时将【加密套件】已选的包含RC4的算法剔除, "验证客户端"不勾选, 并点击【确定】。



4. 调用服务器策略

[FW1]undo ip http enable

```
[FW1]undo ip https enable //调用前先关闭http、https功能  
[FW1]ip https ssl-server-policy https
```