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。

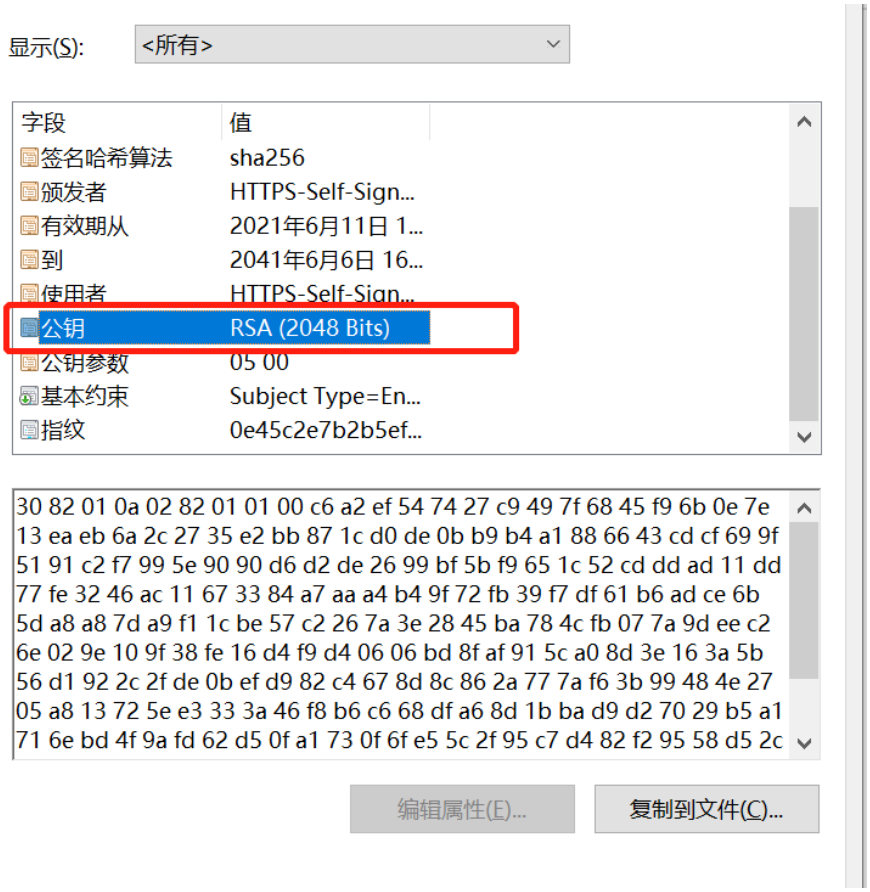
描述：远程主机发送的X.509证书中至少有一个密钥小于2048位。根据认证机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。在2014年1月1日之后，一些浏览器的SSL实现可能会拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销少于2048位的证书。注意，如果RSA密钥在2010年12月31日之前发布，那么Nessus不会将其标记为小于2048位的根证书，因为标准认为它们是豁免的。

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

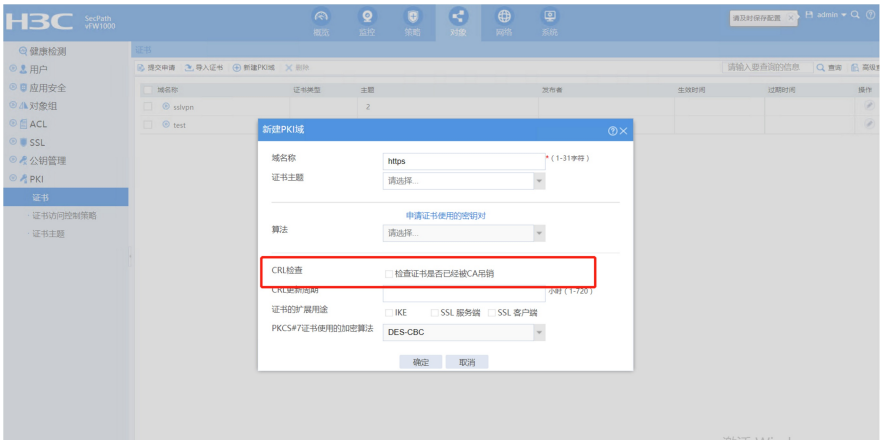
注：仅限于Comware V7的防火墙，导出前确认下该证书是否是2048位。



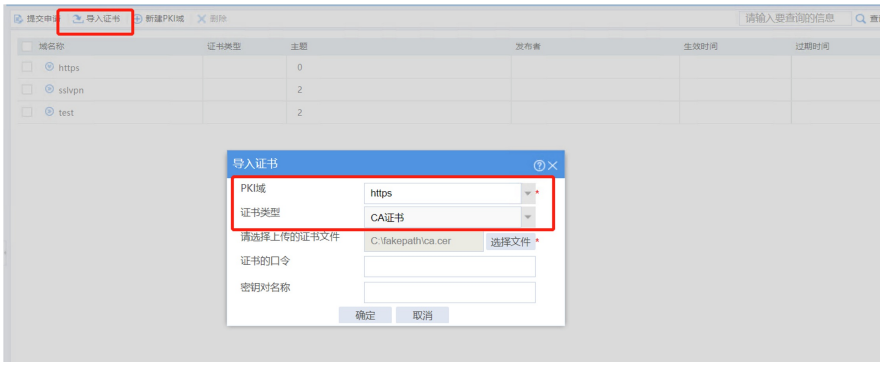
解决方法

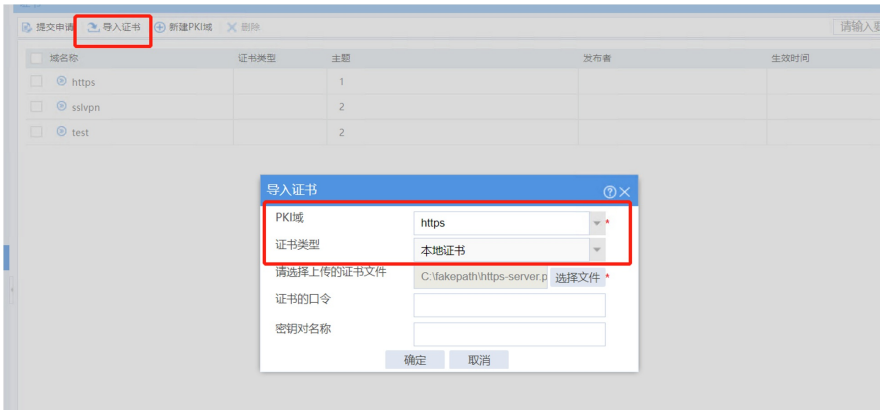
步骤：

1.新建PKI域，命名为https，”检查证书是否被CA吊销“取消勾选

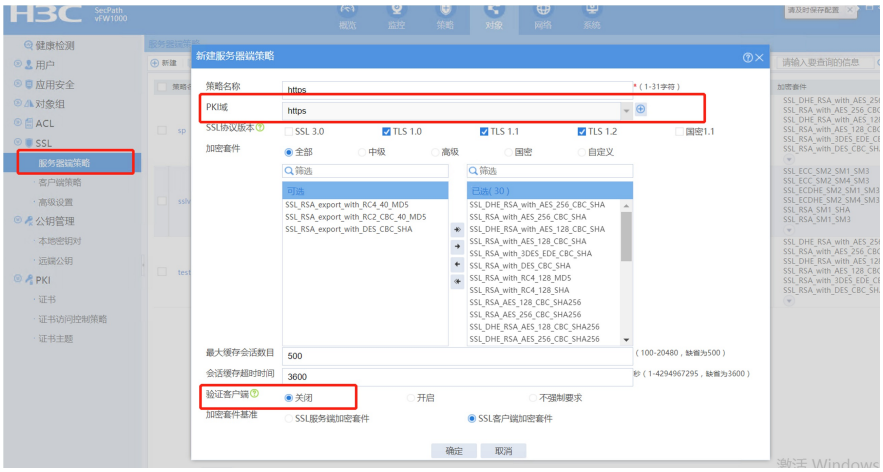


2. 向pki域”https“分别导入CA证书，和本地证书





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