V7产品针对SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)的处理配置方案

wlan安全 朱恺 2017-09-14 发表

客户现场有Comware V7平台无线产品，通过漏洞扫描器发现设备IP地址对外提供SSL服务的端口上存在SSL/TLS受诫礼（BAR-MITZVAH）攻击漏洞（CVE-2015-2808），要求解决该隐患。

SSL/TLS受诫礼（BAR-MITZVAH）攻击漏洞（CVE-2015-2808

SSL/TLS协议是一个被广泛使用的加密协议,Bar Mitzvah攻击实际上是利用了"不变性漏洞"，这是RC4算法中的一个缺陷，它能够在某些情况下泄露SSL/TLS加密流量中的密文，从而将账户用户名密码，信用卡数据和其他敏感信息泄露给黑客。
在V7平台的设备不仅仅是无线控制器开启了HTTPS的web服务，其中就默认支持了RC4的算法，虽然当前主流的新版浏览器都已经正式不支持RC4算法，但是因为设备本身默认开启，对安全敏感性要求较高的用户会提出这方面的要求。

1、首先创建一个SSL Server策略，选择加密套件除去：
[AC2V7]ssl server-policy myssl
[AC2V7-ssl-server-policy-myssl]ciphersuite rsa_aes_128_cbc_sha rsa_des_cbc_sha rsa_3des_ede_cbc_sha rsa_aes_256_cbc_sha exp_rsa_des_cbc_sha dhe_rsa_aes_128_cbc_sha dhe_rsa_aes_256_cbc_sha
2、查看配置状态：
[AC2V7]dis ssl server-policy myssl
SSL server policy: myssl
PKI domain: //默认配置该值为空，因此需要额外配置PKI domain
Ciphersuites:
RSA_AES_128_CBC_SHA
RSA_DES_CBC_SHA
RSA_3DES_CBC_SHA
RSA_AES_256_CBC_SHA
EXP_RSA_DES_CBC_SHA
DHE_RSA_AES_128_CBC_SHA
DHE_RSA_AES_256_CBC_SHA
Session cache size: 500
Caching timeout: 3600 seconds
Client-verify: Disabled

即：
ssl server-policy myssl
pki-domain 1
ciphersuite ……
3、由于pki-domain 1是自己定义的，里面没有任何local 和ca证书绑定关系，在V7 AC上自己已经携带，因此我们要加入绑定的操作
dir查看根目录应该存放了证书
51 -rw- 671 Mar 17 2015 05:19:10 wlan_ca_certificate.cer
52 -rw- 1738 Mar 17 2015 05:19:14 wlan_local_certificate.pfx

[AC2V7]pki import domain 1 der ca filename wlan_ca_certificate.cer
若有提示按Y继续
[AC2V7]pki import domain 1 p12 local filename wlan_local_certificate.pfx
Please input the password: 密码h3c

如果提示
[AC2V7]pki import domain 1 p12 local filename wlan_local_certificate.pfx
Please input the password:
Verify result: unable to get certificate CRL
Failed to verify the local certificates.
Failed to import certificates.
需要关闭CRL检查，然后再绑定一下
[AC2V7]pki domain 1
[AC2V7-pki-domain-1]undo crl check enable

完成绑定之后就能把之前创建的SSL Server策略与PKI domian正确关联上
4、然后禁用当前对外提供的SSL服务，比如HTTPS：
[AC2V7] undo ip https enable
[AC2V7] undo ip http enable
5、配置SSL服务如HTTPS服务应用之前完成的自定义的SSL Server策略：
[AC2V7] ip https ssl-server-policy myssl
6、重新使能SSL服务，开启HTTPS服务
[AC2V7] ip https enable
[AC2V7] ip http enable