

# 知 WX3024H 绿盟扫描安全漏洞问题处理案例

wlan安全 赵杰 2017-09-28 发表

客户购买我司AC部署在内网，通过出口路由器将AC的HTTPS端口映射到2011上，业务运行正常。目前绿盟安全软件扫描AC存在漏洞，导致项目无法验收，求助我司解决问题。

AC型号：WX3024H

软件版本：E5121P21

软件扫描漏洞提示如下：

主机风险		比较危险 (5.1分)	
IP地址		漏洞扫描检查模板	自动匹配扫描
系统版本	V6.0R02F03SP01	漏洞风险评估	5.1分
固件版本	V6.0R02F01.0701	主机风险评估	5.1分
扫描开始时间	2017-09-06 12:42:16		
扫描结束时间	2017-09-06 12:58:53		

  

端口	协议	服务	漏洞	漏洞类别	NF已防护
...	ICMP	..	ICMP网络掩码请求漏洞 ICMP timestamp请求漏洞 允许Traceroute探测	高危漏洞(1)	-
2011	TCP	raid-cc	SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)【原理扫描】 OpenSSL "SSL-Death-Alert" 拒绝服务漏洞(CVE-2016-8610)【原理扫描】 服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)【原理扫描】 SSL/TLS 受减礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】 SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱【原理扫描】 检测到目标服务器支持SSL弱加密算法	高危漏洞(1)	-
			SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】	高危漏洞(1)	-

对于漏洞问题，答复其原意以及解决办法如下：

### 1、SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)【原理扫描】

答复：该问题在V7平台B45版本就已经解决released，V7 AC是B64版本基础之上的不涉及，若还是有风险提示可以尝试命令行关闭SSL3.0即全局：`ssl version ssl3.0 disable`

### 2、OpenSSL "SSL-Death-Alert" 拒绝服务漏洞(CVE-2016-8610)【原理扫描】

答复：该问题V7早期版本都涉及，目前软件已经解决，等待AC版本发布R5213及之后版本，现场升级操作即可。

### 3、服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)【原理扫描】

答复：该问题只需要关闭SSL重协商功能即可，默认开启，命令使用`ssl renegotiation disable`

### 4、SSL/TLS 受减礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】

答复：该问题涉及需要修改SSL使其不支持RC4算法即可，操作命令为：

```
ssl server-policy myssl //创建SSL服务器规则
ciphersuite rsa_aes_128_cbc_sha rsa_des_cbc_sha rsa_3des_edc_cbc_sha rsa_aes_256_cbc
_sha exp_rsa_rc2_md5 exp_rsa_des_cbc_sha dhe_rsa_aes_128_cbc_sha dhe_rsa_aes_256_cbc_s
ha // 默认支持所有算法，当前操作取消RC4支持项
ip https ssl-server-policy myssl //开启设备的https与ssl服务模板绑定。
```

### 5、SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱【原理扫描】

答复：该问题AC的版本分支不涉及

现场工程师修改AC配置之后发现AC不能HTTPS登录，取消`ip https ssl-server-policy myssl`之后可以恢复





在检查SSL-Policy时发现

[AC2V7]dis ssl server-policy myssl //默认配置该值为空，因为https请求发起的时候AC要进行证书确认，因此需要配置PKI domain

SSL server policy:

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

查询到原因后，在设备上创建pki domain，同时在ssl policy下调用domain，同时导入证书：

```
#
pki domain 1
undo cri check enable
#
ssl server-policy myssl
pki-domain 1
```

#

配置完成之后HTTPS重新调用SSL policy之后解决问题。

- 1、修改SSL 算法以及相关功能；
- 2、配置PKI domain，同时导入参数；
- 3、HTTPS重新调用SSL Policy；