

## 知 如何解决设备被扫描出SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞

漏洞 金山 2015-06-26 发表

设备开启SSL/TLS功能后，被漏洞扫描器扫描出存在SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞。

这个问题是由于基础SSL协议策略中，引用了RC4算法。这不是协议的漏洞，而是协议引用的算法造成的。因此，通过修改SSL策略，禁用RC4 算法可解决，使用其它更高级的算法即可解决这个风险。

示例如下：通过修改SSL策略，使其不再包含RC4算法（如红色部分所示）。

```
ssl server-policy default
ciphersuite rsa_des_cbc_sha rsa_3des_edc_cbc_sha rsa_aes_128_cbc_sha
#
return
[H3C]dis ssl server-policy ?
STRING<1-16> SSL server policy name
all      All the SSL server policies
```

```
[H3C]dis ssl server-policy default
```

```
SSL Server Policy: default
```

```
PKI Domain:
```

```
Ciphersuite:
```

```
  RSA_DES_CBC_SHA
```

```
  RSA_3DES_EDE_CBC_SHA
```

```
  RSA_AES_128_CBC_SHA
```

```
Handshake Timeout: 3600
```

```
Close-mode: wait disabled
```

```
Session Timeout: 3600
```

```
Session Cachesize: 500
```

```
Client-verify: disabled
```

```
Client-verify weaken: disabled
```