

知 某局点 S5560-EI/ S6800 CVE 2015-2808 漏洞问题

产品特性 柯辉 2022-06-30 发表

组网及说明

暂无

告警信息

暂无

## 问题描述

现场在5560-EI设备上扫描出 CVE 2015-2808 漏洞，6800未扫描出来

暂无

扫描出漏洞的解决方案为：

**CVE-2015-2808:**

Comware平台可以通过如下方式解决：

1、首先创建一个PKI域：

```
[H3C] pki domain test
```

```
[H3C-pki-domain-test] undo crl check enable
```

(V5命令：crl check disable)

2、在配置视图下通过命令ssl server-policy *policy-name*进入服务器端策略视图，修改SSL加密套件，使其不再包含RC4算法：

```
<H3C>system-view
```

```
[H3C]ssl server-policy test
```

```
[H3C-ssl-server-policy-test]ciphersuite ?
```

```
dhe_rsa_aes_128_cbc_sha
```

```
dhe_rsa_aes_256_cbc_sha
```

```
exp_rsa_des_cbc_sha
```

```
exp_rsa_rc2_md5
```

```
exp_rsa_rc4_md5
```

```
rsa_3des_edc_cbc_sha
```

```
rsa_aes_128_cbc_sha
```

```
rsa_aes_256_cbc_sha
```

```
rsa_des_cbc_sha
```

```
rsa_rc4_128_md5
```

```
rsa_rc4_128_sha
```

```
[H3C]display ssl server-policy test
```

```
SSL server policy: test
```

```
PKI domain:
```

```
Ciphersuites:
```

```
RSA_AES_128_CBC_SHA
```

```
RSA_DES_CBC_SHA
```

```
RSA_3DES_CBC_SHA
```

```
RSA_AES_256_CBC_SHA
```

```
RSA_RC2_CBC_MD5
```

```
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
```

3、引用PKI域：

```
[H3C-ssl-server-policy-test] pki-domain test
```

4、禁用当前对外提供的SSL服务，如HTTPS：

```
[H3C] undo ip https enable
```

```
[H3C] undo ip http enable
```

5、配置SSL服务如HTTPS服务引用前面自定义的SSL Server端策略：

```
[H3C] ip https ssl-server-policy test
```

6、重新使能SSL服务，例如重新使能HTTPS服务：

```
[H3C] ip https enable
```

```
[H3C] ip http enable
```

**重要说明：**

(1) 如果设备开启了SSL VPN功能，需要进入相应的ssl server-policy里面，去除带RC4字段的加密算法，然后进入设备配置的sslvpn context视图重启context服务。

```
[H3C -sslvpn-context-sslvpn]undo service enable,
```

```
[H3C -sslvpn-context-sslvpn]service enable,
```

在系统视图下，重启https服务：

```
[H3C]undo ip http enable
```

```
[H3C]undo ip https enable
```

```
[H3C]ip http enable
```

```
[H3C]ip https enable。
```

(2) 如果设备开启了基于HTTPS的SOAP功能（netconf soap https enable），需要升级至B064D045分支或更高版本，关联SSL Server端策略。

禁用基于HTTPS的NETCONF over SOAP功能：

[H3C] undo netconf ssh enable