

问题描述

端口	协议	服务	漏洞	NPD影响
--	ICMP	--	<ul style="list-style-type: none"> 允许Tracert路由跟踪 ICMP EchoRequest 请求禁止策略 ICMP EchoRequest 请求禁止策略 	-
80	TCP	http	<ul style="list-style-type: none"> 对通过HTTP获取的WWW版本信息 	-
129	UDP	ntp	<ul style="list-style-type: none"> 拒绝非授权方式上送行播NTP消息 	-
832	TCP	netconfsoap	<ul style="list-style-type: none"> 拒绝服务器 TLS Client-initiated 重协商攻击(CVE-2011-1473)【漏洞详情】 SSL/TLS 漏洞:BAR-ABT2044拒绝漏洞(CVE-2015-2048)【漏洞详情】 SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【漏洞详情】 拒绝非授权服务器支持SSL握手结果 拒绝非授权服务器支持SSL握手结果 拒绝非授权方式向服务器支持的加密法 SSL/TLS信息泄露漏洞(CVE-2014-2149)【漏洞详情】 	-

服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)

SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)

解决方法

规避方案:

可以通过配置解决以上漏洞, 具体配置如下:

ssl renegotiation disable 关闭ssl重协商, 解决第1个漏洞: 服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)

ssl version ssl3.0 disable 关闭ssl3.0, 解决第2个漏洞: SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)

需要关闭netconf再重新打开, 上面的ssl配置才能生效, 即

```
undo netconf soap http enable
undo netconf soap https enable
netconf soap http enable
netconf soap https enable
```

注意:

vbrasso有可能导致配置变化, 也就是有可能会业务中断。

Netconf断开后重连, vbrasso会对vbras进行配置平滑, 所以需要提前将vbras的配置保存在本地电脑上, 等vbrasso重新连接上之后, 再检查当前配置与电脑上保存的配置是否相同, 再手动将不同的地方修改一致