VBRAS 832端口漏洞规避方法

NETCONF 吕甲南 2019-04-17 发表

问题描述

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，也就是有可能会导致业务中断。
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