中低端路由器 CVE-2011-1473漏洞处理方法（SDWAN场景）

软件相关 王科 2023-07-29 发表

问题描述

我司中低端路由器设备被第三方安全设备扫描出漏洞：服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)。

解决方法

1. 如果是非SDWAN环境，参考此链接处理方法：https://zhiliao.h3c.com/Theme/details/195514
2. SDWAN环境下，若是客户使用漏扫平台检查在网的sdwan设备，发现设备都因SDWAN服务端口号(例如1234)开放监听导致被扫描到此漏洞。按照如下方法解决：

检查设备上的配置是否有 ssl renegotiation disable，如果没有，需要配置后，重启sdwan server服务，操作步骤：如下。

1） ssl renegotiation disable

2） undo sdwan server enable

3） sdwan server enable

需注意，此修改可能会导致分支和总部之间的业务中断，请谨慎操作。同时需注意，ssl renegotiation disable操作会增加开销。

ssl renegotiation disable命令用来关闭SSL重协商。

undo ssl renegotiation disable命令用来恢复缺省情况。

【命令】

ssl renegotiation disable

undo ssl renegotiation disable

【缺省情况】

本命令的缺省情况与设备的型号有关，请以设备的实际情况为准。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【使用指导】

关闭SSL重协商是指，不允许复用已有的SSL会话进行SSL快速协商，每次SSL协商必须进行完整的SSL握手过程。**关闭SSL重协商会导致系统付出更多的计算开销，但可以避免潜在的风险，安全性更高。**

通常情况下，不建议关闭SSL重协商。本命令仅用于用户明确要求关闭重协商的场景。

【举例】

关闭SSL重协商。
<Sysname> system-view
[Sysname] ssl renegotiation disable

PS：设备的安全增强级别有两个，分别为1和2，2的安全级别较高。当设备的安全级别为2时，默认开了“关闭重协商”配置（既**ssl renegotiation disable**），不支持开启SSL重协商功能。security-enhanced level命令用来配置设备的安全增强级别。本命令的缺省情况与设备的型号有关，请以设备的实际情况为准。

```
security-enhanced level 2
#
 ssl version gm-tls1.1 disable
 ssl renegotiation disable
 ssl version ssl3.0 disable
 ssl version tls1.0 disable
 undo ssl version tls1.1 disable
 undo ssl version tls1.2 disable
 undo ssl version tls1.3 disable


security-enhanced level 1
#
 undo ssl renegotiation disable
 undo ssl version ssl3.0 disable
 ssl version gm-tls1.1 disable
 undo ssl version tls1.3 disable
 undo ssl version tls1.0 disable
```

undo ssl version tls1.1 disable
undo ssl version tls1.2 disable