应用场景

硬件/整机信息：全平台

OS版本信息：桌面专业版102X

软件信息：openssh

问题现象

专业版102X版本默认启用ssh服务同时使用22端口通信，此服务存在一定的弱点，当配置为特定模式例如采用默认的标准端口时会非常容易成为网络远程攻击的对象。

解决方案

建议终端用户对旧版本的专业版102X版本相关ssh服务采用下列调整方案，可根据现场实际用户场景从下列可选方案中选择任意一种进行调整即可解决ssh服务安全隐患：

方案一：关闭相关服务

开启开发者模式后，在终端中手动执行如下指令：

uos@uos-PC:~$ sudo systemctl stop ssh && systemctl stop sshd

uos@uos-PC:~$ sudo systemctl disable ssh && systemctl disable sshd

上述指令执行完毕后建议执行标准操作重启系统，用以正常关闭当前已登录的ssh连接。

方案二：Udom工具箱

通过应用商店安装”Udom工具箱“：



通过启动器中的udom工具箱启动图标运行此工具：



通过”关闭SSH远程功能“工具，可较便捷的实现服务调整：



小程序运行完毕后会出现服务关闭执行完毕的反馈信息，然后正常退出工具箱即可：



相关说明

* 升级系统无法自动关闭ssh服务，即通过“控制中心“的”更新“按钮升级系统到主线最新版本仍会保持原有的默认配置；
* 新版本系统纯净安装场景下，系统会默认关闭ssh服务。

©统信软件技术有限公司。访问者可将本网站提供的内容或服务用于个人学习、研究或欣赏，以及其他非商业性或非盈利性用途，但同时应遵守著作权法及其他相关法律的规定，不得侵犯本网站及相关权利人的合法权利。除此以外，将本网站任何内容或服务进行转载，须备注：**该文档出自【faq.uniontech.com】统信软件知识分享平台**。否则统信软件将追究相关版权责任。