UNIS XSCAN-CN60 漏洞扫描系统

故障处理手册

目 录

1 简介

本文档介绍 UNIS XSCAN-CN60 漏洞扫描系统常见故障的诊断及处理措施。

本文档适用于用户、系统管理员在产品使用过程中出现的故障处理及注意事项。

注意

系统正常运行时，建议您在添加任务后，请勿进行关机重启等操作，以免影响其它用户正在执行的任务，避免造成任务中断，任务停止，影响其它用户使用。

1.1 故障处理注意事项

注意

设备正常运行时，建议您在完成重要功能的配置后，及时保存并备份当前配置，以免设备出现故障后配置丢失。建议您定期将配置文件备份至远程服务器上，以便故障发生后能够迅速恢复配置。

在进行故障诊断和处理时，请注意以下事项：

- 系统出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），收集信息越全面、越详细，越有利于故障的快速定位。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障时间，故障功能模块。
  - 查看系统信息和诊断信息。
  - 记录设备故障时单板、电源、风扇指示灯的状态，或给现场设备拍照记录。
  - 记录现场采取的故障处理措施和后台执行操作（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
  - 记录故障处理过程中配置的所有命令行显示信息。
- 更换和维护设备部件时，请关机并摘除电源以确保您和设备的安全。
- 故障处理过程中如需更换硬件部件，请参考与软件版本对应的版本说明书，确保新硬件部件和软件版本的兼容性。

1.1 故障处理求助方式

使用过程中，常见故障问题，请参考以下故障处理解决办法，若您遇到的问题不在以下故障处理范围内，或者当故障无法自行解决时，请详细记录故障信息、故障现象等，并和 UNIS 技术支持人员沟通，进行故障定位分析，获取解决办法。

用户支持邮箱：service@unis.com

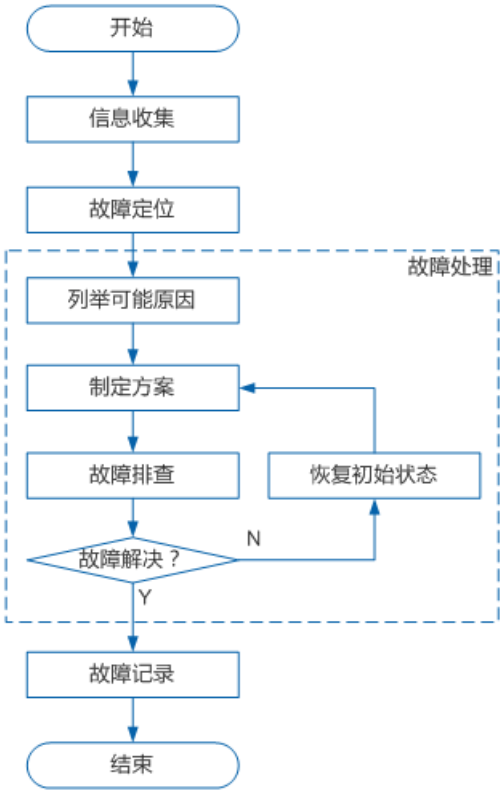
技术支持热线电话：400-910-9998（手机、固话均可拨打）

1.2 故障处理流程

故障的处理难以根据现象直接推导出故障原因，不同原因可能会导致相同的故障现象。本节提供的故障处理流程主要用于指导用户科学地处理故障，有效地将故障范围缩小。从而达到提高故障处理效率，减少处理时间的目的。

系统化的故障处理，有利于将大型、综合、复杂的现象分隔缩小范围，从而达到对故障现象的准确定位。

图1-1 故障处理流程



- 信息收集：发生故障后应该第一时间收集故障的相关信息，而不是盲目的进行故障恢复。
- 故障定位：根据收集的故障信息，进行故障的初步定位，从而有效的缩小故障的范围。
- 列举可能原因：根据定位后的结果，列出所有的可能原因。
- 制定方案：以故障原因的可能性大小，辅助参考是否容易实施，制定故障排查的顺序，同时每种原因也要制订故障排查方案。
- 故障排查：按照方案依次进行故障的排查，根据排查结果决定是否继续排查下一个原因。
- 恢复初始状态：在排除特定故障后，如果没有解决问题，需要恢复为故障的初始状态，避免引入其它故障。
- 故障记录：完成故障处理后，需要将故障排查过程进行文档化记录，以便故障排查经验的记录和传递。

1.3 了解故障相关的其它信息

从受故障影响的用户收到报告，并收集到一些故障现象后。还需要从其它相关用户那里继续收集有用的信息，以辅助进行定位判断。通常需要确认：

(1) 发生故障时是否修改了配置？

(2) 设备在正常情况下的工作状态？

(3) 发生故障前，用户可能做了哪些操作，操作的顺序是怎样的？

1.4 故障记录

将故障处理的过程进行文档化是故障处理的最后一步，完整清晰的文字记录有助于对故障处理经验的积累和传递。记录中需要包含本次故障处理的全部信息，通常包含：

(1) 故障现象描述及收集的相关信息。

(2) 网络拓扑图绘制。

(3) 故障发生的可能原因。

(4) 对每一种可能原因制定的方案和实施结果。

2 系统维护

2.1 系统升级

2.1.1 系统升级方式

登录 account 账户，选择**系统管理>版本/版本库升级>版本/版本库升级**；或者使用 SSH 工具登录系统后台，使用命令进行升级。

(1) 自动升级

(2) 手动升级

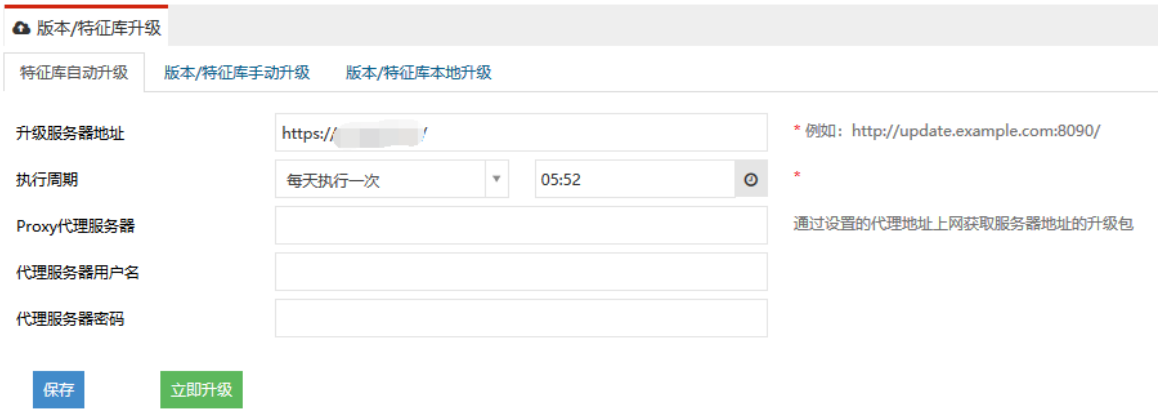
(3) 本地升级

(4) 命令行升级

2.1.2 系统升级步骤

(1) 自动升级，account 登录 Web 界面选择**系统管理>版本/版本库升级**，点击“立即升级”。自动升级只能升级规则库，不能升级系统版本。

图2-1 自动升级规则库



(2) 本地升级

点击导入的按钮，选择本地的升级文件直接导入即可。

图2-2 本地升级

(3) 手动升级，手动升级需要把升级固件文件或者规则库文件存放在本地，并在本地搭建 FTP 环境(如 FTP 环境软件 3CDaemon)

在本地搭建 ftp（3CDaemon 软件）环境，关闭本地主机防火墙，选择对应的升级路径和文件，进行升级。

命令：ftp://user:pass@ip:port/包名.img

图2-3 FTP 环境

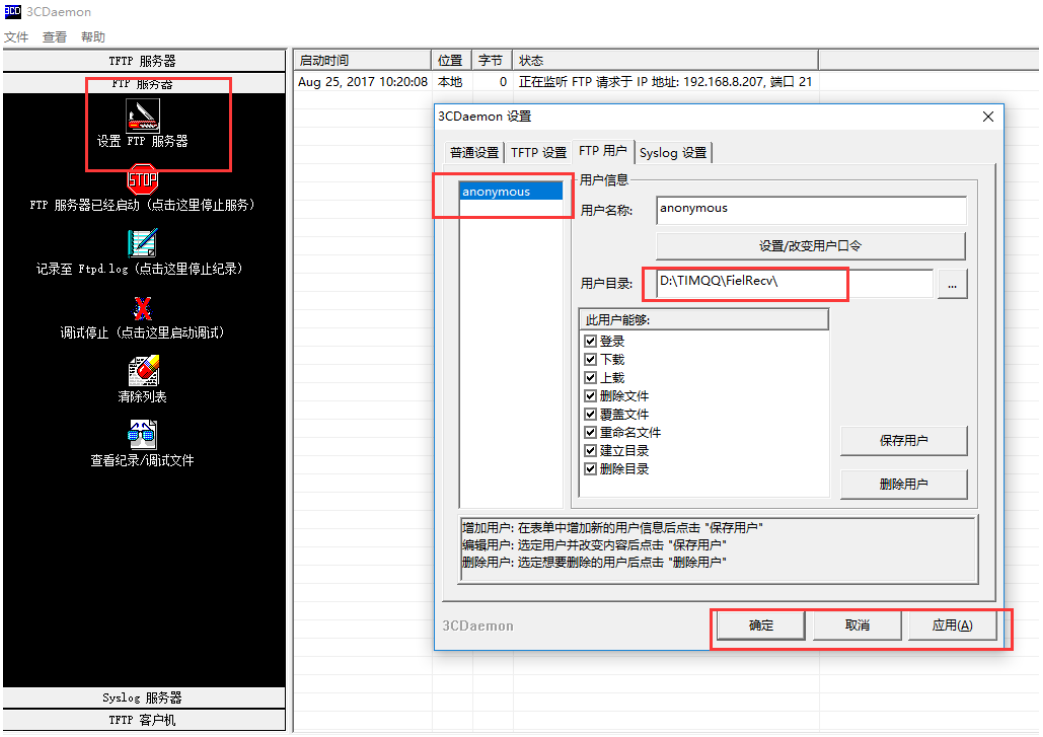


图2-4 手动升级

(4) 后台升级

打开 SSH 访问软件如 Xshell，使用 ssh2 协议登录后台，身份验证方法选择 Keyboard Interactive，用户名/密码：admin/admin

本地搭建 ftp（3CDaemon 软件）环境，关闭本地主机防火墙，选择对应的升级路径和文件。

后台执行命令：

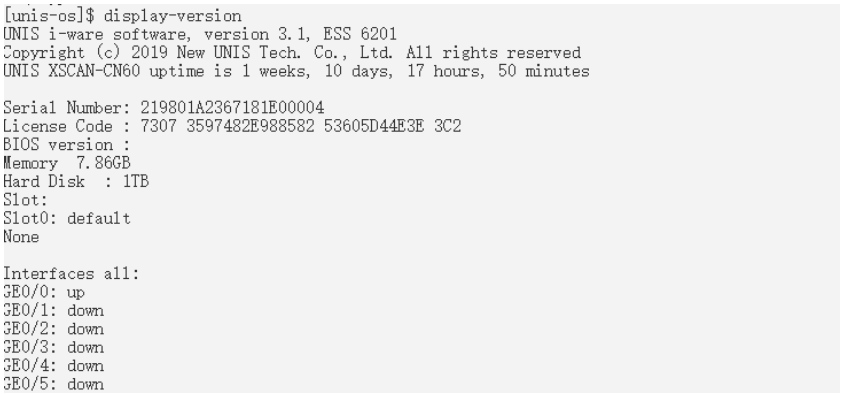
规则库升级：sigup ftp://ip/包名.img

固件：patchall ftp://ip/包名.img

2.2 查看系统信息

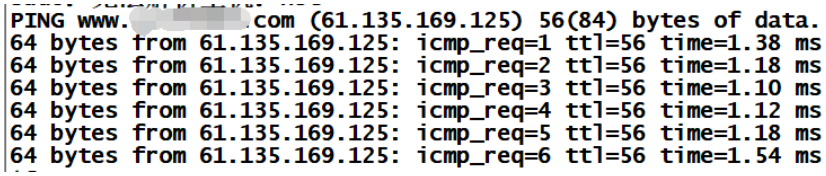
2.2.1 使用 SSH 工具登录后台，执行命令 display-version 查看当前系统信息。

图2-5 系统信息



2.2.2 使用 SSH 工具登录后台，执行命令 ping 测试网络状况。

图2-6 网络状况诊断



3 故障处理

3.1 漏洞扫描无结果

3.1.1 故障描述

在执行完扫描任务后查看扫描结果，扫描没有结果。添加任务进行扫描后，扫描无结果，漏洞数为0。

3.1.2 故障处理流程

(1) 确认扫描网站信息填写无错误。

(2) 确认设备和被扫描网站网络互通。

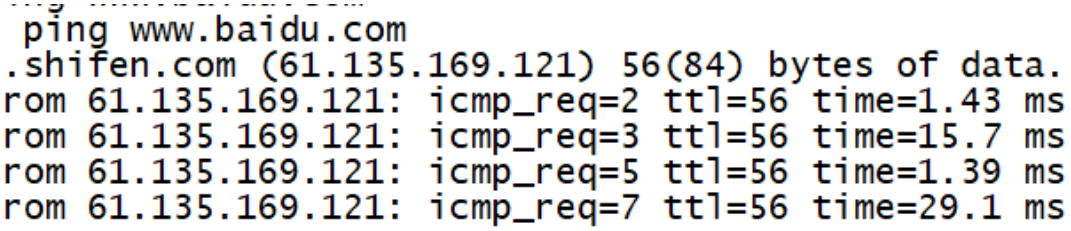
3.1.3 使用网站登录扫描。故障处理步骤

(1) 此类问题多数是因为通信网络问题导致的，用户需诊断平台是否可与站点正常通信，如果诊断没问题则证明通信正常，这时可能是因为站点上加了防护设备，对平台的流量进行拦截造成的，建议检查站点是否有防护设备，然后将平台的 IP 加入防护设备白名单来解决此问题。

(2) 在**系统管理>诊断工具**或者使用 SSH 工具登录设备后台，登录成功后使用 ping 命令进行诊断，以 ping www.baidu.com 示例，可访问则需要排除防护设备的影响，可咨询相关客户技术人员。

图3-1 诊断测试

图3-2 诊断测试



3.2 用户忘记密码或用户被锁定。

3.2.1 故障描述

Web 界面登录用户，提示账户被锁定，请联系管理员。

图3-3 用户名被锁定

图3-4 用户名被锁定

3.2.2 故障处理流程

管理员使用 account 管理员登录后找到对应的用户，解除锁定或者重置密码。

3.2.3 故障处理步骤

图3-5 解锁或者重置用户

问题是由于账户登录时，输入错误的密码超过限定次数后导致。account 管理员 Web 登录，选择**系统管理>账号管理>用户管理**，解锁被锁定账户即可。重置密码后密码和用户名相同。

3.3 设备无法开机

3.3.1 故障描述

设备上线加电，指示灯全部不亮，风扇不转

3.3.2 故障处理流程

(1) 未打开电源开关。
(2) 设备的输入电源又故障。
(3) 设备本身的电源模块有故障。

3.3.3 故障处理步骤

(1) 确认是否未打开设备电源或供电电源的开关。
(2) 通过使用其它可以正常供电的电源输入，替换出现故障的线路。
(3) 如果可以正常供电，可以确认是外部输入电源有故障。
(4) 如果使用其它可以正常供电的电源输入，设备仍然不能正常上电。可以确认是设备本身电源模块有故障，请与售后服务工程师联系。

3.4 风扇故障

3.4.1 故障描述

设备加电后没听到风扇转动的声音或者没看到风扇转动。

3.4.2 故障处理流程

(1) 未安装风扇或风扇电源接头接触不好。
(2) 风扇被物体卡住或灰尘较多导致堵转。
(3) 风扇内部故障。

3.4.3 故障处理步骤

(1) 查看设备风扇是否存在，或风扇是否插牢。
(2) 如果没有风扇，请与售后服务工程师联系。有风扇且设备为分布式设备，可以尝试重新插拔一下风扇框。
(3) 如果风扇在位，但是上电后不转。请检查风扇是否被物体卡住；如果是可插拔风扇，检查是否安装牢固。
(4) 如果风扇被卡住，请小心取出卡住风扇的物体。
(5) 以上故障均排除后，可以判断为风扇内部故障。请与售后服务工程师联系。

3.5 浏览器打开地址链接显示证书存在安全问题

3.5.1 故障描述

浏览器访问平台链接地址后，提示此证书存在安全问题。

图3-6 浏览器访问证书问题

图3-7 浏览器访问证书问题

3.5.2 故障处理流程

点击继续前往即可。

3.5.3 故障处理步骤

点击“继续跳转到网页”、“继续前往”按钮即可。

3.6 登录后提示许可证到期

3.6.1 故障描述

登录系统无其它功能菜单项，只有许可证管理栏，显示许可证不可用。提示该信息代表您的授权为测试版授权。

3.6.2 故障处理流程

导出授权文件发送给 UNIS 工程师，并接收许可文件导入。

3.6.3 故障处理步骤

页面右上角点击导出许可文件，导出许可文件到本地，然后联系 UNIS 工程师，发送导出文件后，待接收新的授权文件并导入。

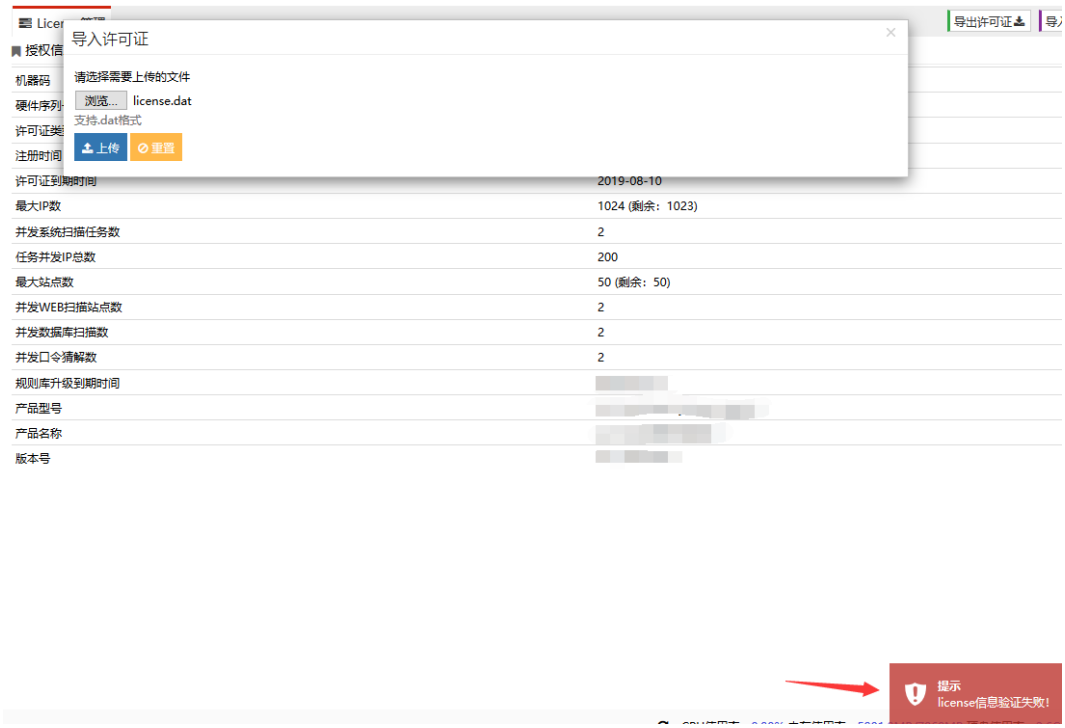
图3-8 许可证管理

3.7 License升级失败

3.7.1 故障描述

升级 License 失败。在许可证管理中，选择“导入许可证”，上传许可证后显示 License 验证失败。

图3-9 升级 License 失败



3.7.2 故障处理流程

由于 License 不正确导致的，可能由于设备与授权步匹配导致。

3.7.3 故障处理步骤

License 不正确导致的，请联系售后工程师获取正确的 License 或者确认 License 文件是否有混淆。

3.8 升级License后不生效。

3.8.1 故障描述

License 上传成功后，没有生效。

3.8.2 故障处理流程

(1) 刷新浏览器页面重新进查看授权信息。

(2) 重新升级授权许可。

3.8.3 故障处理步骤

(1) 1-2 分钟后刷新浏览器页面重新进入系统查看授权信息。

(2) 使用谷歌浏览器或者火狐的浏览器重新升级授权许可。

3.9 Web扫描有页面无漏洞

3.9.1 故障描述

对网站进行扫描后无结果，无漏洞。

3.9.2 故障处理流程

(1) 被扫描的 Web 网站应用本身无漏洞。

(2) 发探测包去解析和测试的时候被防护设备拦截。

(3) 发攻击包的前提是根据爬到的页面发对应的攻击包，所以爬不到页面也就不会发攻击包，不会去检测漏洞。

(4) 页面数太多，但没有漏洞，原因是超过扫描超时停止时间，自动断开，还未判断出漏洞任务被自动结束。

3.9.3 故障处理步骤

(1) 查看当前页面数和任务，并根据当前任务进程判断是否是由于任务超时导致。一般检测时间过长超过 10 小时以上有页面数无漏洞结果，极可能是任务超时退出导致。

3.10 系统扫描无结果结束

3.10.1 故障描述

在添加多个系统扫描任务后，没有任何扫描结果后自动结束扫描任务。

3.10.2 故障处理流程

在添加多个系统扫描任务后，没有任何扫描结果后自动结束扫描任务。

3.10.3 故障处理步骤

(1) 解决网络的连通性问题使扫描器到被扫描目标网络可达。

(2) 安全防护设备上拔扫描器的 IP 地址加白名单。

(3) 使用强制扫描，关闭主机存活探测。

3.11 Web界面无法管理，SSH可访问设备22端口

3.11.1 故障描述

图3-10 找不到服务器

3.11.2 故障处理流程

重启 httpserver 服务。

3.11.3 故障处理步骤

图3-11 重启 httpserver 服务

```
[ ]$ httpserver restart
httpserver restart success
[ ]$
```

使用 SSH 工具，登录系统后台 22 端口，用户名 admin，密码 admin，登录成功后执行命令 httpserver restart，然后重新在浏览器访问。

3.12 告警接收异常

3.12.1 故障描述

告警邮件已发出，但是用户未接收到告警信息。

3.12.2 故障处理流程

(1) 判断设备是否可访问外网。

(2) 检查邮箱是否已满，是否将告警邮箱标记为垃圾邮件。

(3) 检查邮箱名称是否正确。

(4) 发送测试邮件，看是否能收到；并使用其它邮箱进行发送。

3.12.3 故障处理

(1) 判断设备是否可访问外网。

(2) 清理邮箱的文件存储空间，设置发件人邮箱设置白名单。

(3) 填写正确的邮件服务器信息。

(4) 使用独立的邮箱发送告警邮件，该配置代表使用此邮箱（如 163 邮箱等）来给接收者发送告警邮件。

图3-12 修改邮箱配置

3.13 常用故障诊断命令

命令	说明
help	帮助按钮
display-version	系统版本信息
port	接口和vlan状态信息
httpserver	Web服务进程 命令格式：httpserver restart
syseng_status	显示扫描引擎状态
syseng_restart	重启扫描引擎
patchall	固件升级命令 命令格式： • 示例：patchall http://192.168.1.1/xxx.img 从 http 服务器 192.168.1.1 上获取固件升级包并升级 • 示例：patchall ftp://192.168.1.1/xxx.img 从 ftp 服务器 192.168.1.1 上 获取固件升级包并升级
sigup	规则库和补丁升级

	命令格式： • 示例：sigup http://192.168.1.1/xxx.img 从 http 服务器 192.168.1.1 上获取规则库升级包或补丁并升级 • 示例：sigup ftp://192.168.1.1/xxx.img 从 ftp 服务器 192.168.1.1 上获取规则库升级包或补丁并升级
ping	Ping命令主要用于检查网络连接及主机是否可达
tcpdump	Linux中强大的网络数据采集分析工具之一，以将网络中传送的数据包完全截获下来提供分析