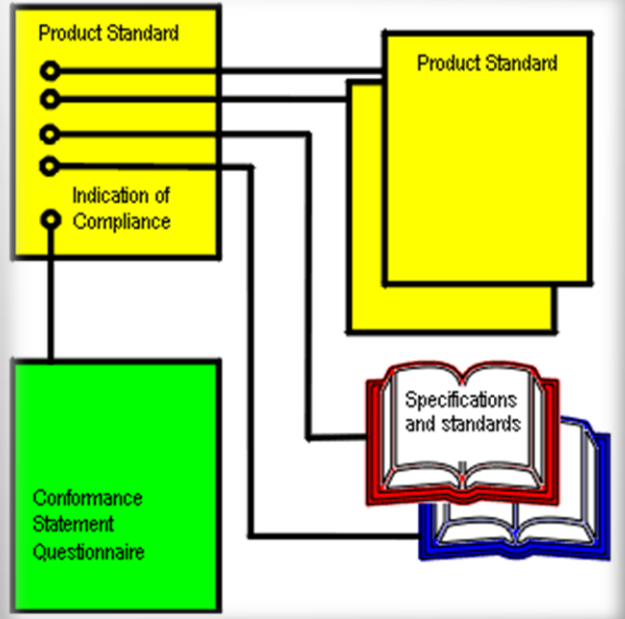
硬件产品安全规范

李伟，常涛

2016年10月27@安全文档

目录

- 产品红线
- 安全问题通知流程
- 安全问题的处理时间



产品红线-原则

1. 符合集团红线要求
2. 添加符合萤石产品需求的要求

产品红线-细则

NU	需求分类	需求名称	需求描述
1	禁用不安全协议	禁用 telnet 服务	所有禁止提供telnet服务，原则上要求在通过裁剪操作系统服务的形式，在提供的固件中删除telnet的相关代码和模块，确保任何情况下telnet都是无法启用的（包括缓冲器溢出）。
		禁用 ftp 服务	同“禁用 telnet 服务”的安全措施
2	主动监听的端口	使用端口白名单的机制	所有主动开启并且监听的端口，必须要有文档记录，并且说明端口的使用情况和端口通信的认证条件和认证过程，认证条件和认证过程必须通过安全团队测试和评估。
		非白名单端口必须关闭	不在白名单记录内的端口必须关闭。
3	秘钥要求	初始秘钥策略	1，确保初始秘钥的不可预测性和随机性； 2，无法确保“1”的情况下，只要用户在设置自己的秘钥之后才能正常使用产品；
		秘钥提醒策略	1，产品必须提醒用户设置负责密码；
		秘钥存储和传输策略	1，禁止一切明文传输和存储秘钥的行为；
		秘钥复杂度策略	1，秘钥长度不得低于6个字符； 2，秘钥必须包含，数字，大写字母，小写字母，特殊符号，中的两类；
4	认证要求	认证功能	1，互联网可以访问的接口必须具有认证能力；
		防止暴力破解能力	1，互联网可以访问的通过密码认证的接口都需要防止暴力猜测密码的能力；

IPC开放端口白名单

NU	协议:端口号	端口作用	认证方式和认证的条件(访问这个接口需要满足的条件)
1	TCP:RTSP:554		
2	TCP:RTP:8200		
3	TCP:8000	NetSDK协议端口	
4	TCP:9010		
5	TCP:9020		
6	TCP:7001	本地回路端口	
7	TCP:50100	互联互通监听端口	
8	UDP:9030-9033	P2P直接链接	
9	UDP:10000-10800	P2P 3/4组合打洞时，会临时监听多个UDP端口	依赖于DAS和设备之间同步的加密key来完成认证。

后端开放端口白名单

NU	协议:端口号	端口作用	认证方式和认证的条件(访问这个接口需要满足的条件)
1			
2			
3			
4			
5			
6			
7			
8			
9			

安全问题通知流程

- 核心思想：必须收到反馈
- 通信收到：
  - 手机
  - 短信
  - 邮件

安全问题的处理时间

- 开发在收到安全问题的反馈的时候必须在24小时之内做出响应。