网络设备安全需求规格书



2013年月日发布 2013年月日实施

华为技术有限公司

Huawei Technologies Co., Ltd.

版权所有侵权必究

All rights reserved

修订声明Revision declaration

拟制与解释部门：

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 主要起草部门专家 | 主要评审部门专家 | 修订情况 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

网络设备安全需求规格书

# 安全性规格

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **子项目** | **需求规格** |
| 1 | 管理通道安全 | 管理面与用户面隔离 | a) 如果设备仅支持带外管理的系统，系统必须保证管理面与用户面隔离，确保在用户面使用端口扫描工具（如nmap）无法扫描到管理平面的地址及端口。  b) 对于支持带内管理模式且有独立管理面IP的设备，设备应提供有效的办法（如ACL、VLAN等机制）来保证带内管理面与用户面的隔离。  [会议讨论]支持带外管理，不实现Vlan，ACL机制。 |
| 2 | 操作系统安全 | 操作系统生命周期 | 不得使用已经停止维护的操作系统版本。 |
| 操作系统加固 | 1、系统经业界主流漏洞扫描工具扫描（如Nessus），扫描报告中不得出现高风险级别的漏洞。  [会议讨论]A类需求，需要满足。Nessus为商用工具  2、系统提供安全配置/加固指南和安全维护手册等文档。 |
| 物料对操作系统安全补丁的兼容性测试 | 需要制定周期性安全预警、安全补丁发布计划，安全补丁要提供兼容性测试报告。建议每季度发布一次补丁。  [会议讨论]嵌入式设备可以通过系统升级实现 |
| 3 | Web系统安全 | 登录认证防暴力破解 | 登录认证模块提供防暴力破解机制：验证码或者多次连续尝试登录失败后锁定帐号或IP |
| 会话管理 | 对于每一个需要授权访问的页面或servlet的请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作，以防止URL越权。 |
| 登录口令保护 | 向服务器端传递用户名和口令（含应用层用户名/口令）时，需采用安全协议（如HTTPS、HTTP digest）或加密用户名/口令后再传输。 |
| 认证管理 | 对用户的最终认证处理过程必须放到服务端进行。 |
| 输入校验 | 系统外部输入需在服务端进行最终校验。 |
| 输出编码 | 对于不可信的数据，输出到客户端前必须先进行HTML编码。  [会议讨论]A类需求，需要满足。防止脚本注入攻击。 |
| Web系统漏洞 | 提供使用Web安全扫描工具（如AppScan、WebInspect、Acunetix Web Vulnerability Scanner）扫描的报告，扫描报告中不得出现高风险级别的漏洞。  [会议讨论] A类需求，需要满足 |
| 4 | 产品开发、发布和安装安全 | 禁止绕过系统安全机制的功能 | 1、禁止隐秘访问方式：包括隐藏账号、隐藏口令、隐藏模式命令/参数、隐藏组合键访问方式；隐藏的协议/端口/服务；隐藏的生产命令/端口、调测命令/端口；不记录日志的非查询操作等  2、禁止不可管理的认证/访问方式：包括用户不可管理的帐号，人机接口以及可远程访问的机机接口的硬编码口令，不经认证直接访问系统的接口等。  3、除上述隐秘、不可管理的认证/访问方式外，不得含有其它任何形式的后门、木马等恶意代码或未知功能。 |
| 禁止存在未文档化的命令/参数、端口等 | 1、不得存在客户资料中没有公开的协议端口/服务；  2、不得存在未文档化的命令、参数等（包括但不限于产品的生产、调测、维护用途） |
| 软件完整性 | 对于涉及软件包分发的物料应提供完整性校验机制（如：数字签名或者哈希值），并提供文档说明验证方法。  注：CRC不能用于完整性校验。 |
| 5 | 协议与接口 | 通信矩阵 | 1、提供清单列举物料所有功能/特性所使用到的端口；  2、如存在动态侦听端口，侦听范围必须限定在确定的必要的范围内；  3、未在通信矩阵中描述的端口应关闭 |
| 协议安全 | 1、系统的管理平面和近端维护终端（如LMT）、网管维护终端间，支持使用合适的安全协议（如SSH v2/TLS1.0/SSL3.0/IPSec/SFTP/SNMPv3等）进行通信。  2、对于不安全协议（如FTP、Telnet），支持关闭，建议缺省关闭。产品资料中应建议用户使用安全协议，如需使用不安全协议，应提示风险。 |
| 端口接入认证 | 能对系统进行管理的逻辑端口/协议，应提供接入认证机制，标准定义无认证机制的除外。 |
| 协议健壮性 | 对与终端用户有交互或者与非信任网络互联的容易受攻击的协议，使用Codenomicon Defensics工具或华为认可的具有同等能力的工具进行畸形报文攻击测试，测试结果不得出现致命或严重级别的问题。  [oplink] A类需求，需要满足。Codenomicon Defensics为商用工具。  这些协议和版本包括但不限于*（请去掉产品无关的协议、补充相关的协议）*：  BGP, Diameter, DNS, DVRMP, EAP, FTP, GRE, GTP, H.225, H.248, H.323, HTTP, ICMP, IMAP, IPSec, IPv4, IPv6, IS-IS, ISAKMP/IKE, LDAP, MGCP, MPLS/LDP, NTP, OSPF, PIM, POP3, RADIUS, RIP, RSVP, RTP, RTSP, SIGCOMP, SIP, SNMP, SMTP, SSH, SSL/TLS, TACACS, TR-069, XML/SOAP, WAP. |
| 物理接口接入认证 | 在设备面板上可见的能对系统进行管理的物理接口，应提供接入认证机制。 |
| 6 | 敏感数据与加密 | 加密算法清单 | 提供使用的所有加密算法清单，说明加密算法的应用场景。 |
| 私有密码算法 | 禁止使用私有算法实现加解密，包括但不限于：  1. 自行定义的通过变形/字符移位/替换等方式执行的数据转换算法。  2. 使用非密码算法用于加密目的，如用编码的方式（如Base64编码）实现数据加密的目的的伪加密实现。 |
| 不安全密码算法 | 禁止使用当前已知的不安全的密码算法（如DES、RC2）；不建议使用存在安全风险的密码算法（如：MD5、SHA-1、RSA1024）。因标准协议定义且没有替代算法、需要与第三方系统对接、兼容老系统等情况需要使用不安全密码算法的，应在加密算法清单中说明。  [oplink]推荐使用的加密算法为 对称加密AES-256和非对称加密SHA-256 |
| 敏感数据存储安全 | 口令不允许明文存储在系统中，应该加密保护。在不需要还原口令的场景，必须使用不可逆算法加密。对银行账号等敏感数据的访问要有认证、授权和加密机制。 |
| 敏感数据传输安全 | 在非信任网络之间进行敏感数据（包括口令，银行帐号，批量个人数据等）的传输须采用安全传输通道或者加密后传输，有标准协议规定除外。 |
| 密钥安全 | 用于敏感数据传输加密的密钥，不能硬编码在代码中。 |
| 7 | 个人数据（隐私）保护 | 个人数据转移 | 1、不得未经用户授权对外传送用户的个人数据，传送功能/特性应允许关闭；  2、对外传送个人数据的类型、目的、实现和管理机制应在资料中公开。 |
| 个人数据采集/处理 | 涉及个人数据采集/处理的功能须提供安全保护机制（如访问控制、加密、日志审计等），并在资料中公开个人数据类型、目的、安全保护机制。 |
| 精准位置信息 | 1、提供物料所涉及到的最终用户精准位置信息清单，说明精准位置信息的应用场景；  2、禁止出于故障定位目的进行用户精确位置信息定位。 |
| 8 | 口令安全 | 口令复杂度检查 | 口令应默认检测口令复杂度，口令至少满足如下要求：  1、口令长度至少6个字符（特权用户至少8个字符）；  2、口令必须包含如下至少两种字符的组合:  －至少一个小写字母；  －至少一个大写字母；  －至少一个数字；  －至少一个特殊字符：`~!@#$%^&\*()-\_=+\|[{}];:'",<.>/? 和空格  3、口令不能和帐号或者帐号的倒写一样；  若设置的口令不符合上述规则，必须进行警告。 |
| 用户锁定机制 | 支持设置口令出错锁定阈值，提供锁定用户的机制。  参考机制：  方式一：当重复输入错误口令次数（默认3次，次数系统可以设置）超过系统限制时，系统要锁定该用户。  方式二：系统还可以设置下次允许输入口令的间隔时间加倍，采用这种方式时，用户可以不设置自动锁定。 |
| 口令加密存储 | 1、口令不能够明文写入日志文件、配置文件以及cookie中；  2、口令文件必须设置访问控制，普通用户不能读取或拷贝加密的内容。 |
| 口令安全传输 | 提供传送口令的安全通道，保证口令不明文在网络中传送 |
| 账号口令清单 | 提供账号口令清单。 |
| 9 | 日志审计 | 管理面所有的用户活动、操作指令必须记录日志 | 涉及以下用户活动和操作指令的需要记录日志：  用户活动包括：  1、登录和注销；  2、增加、删除用户和用户属性（帐号、口令等）的变更；  3、用户的锁定和解锁，禁用和恢复；  4、角色权限变更；  5、系统相关安全配置（如安全日志内容配置）的变更；  6、重要资源的变更，如某个重要文件的删除、修改等。  操作指令包括：  1、对系统配置参数的修改；  2、对系统进行启动、关闭、重启、暂停、恢复、倒换；  3、对业务的加载、卸载；  4、软件的升级操作，包括远程升级和本地升级；  5、对重要业务数据（特别是与财务相关的数据，包括：卡号、余额、话单、费率、费用、订单、出货、帐单等）的创建、删除、修改；  6、所有帐户的命令行操作命令。 |
| 日志内容要能支撑事后的审计 | 日志内容要能支撑事后的审计，记录包括用户ID、时间、事件类型、被访问资源的名称、访问结果等。 |
| 日志要有访问控制、 | 1、日志要有访问控制；  2、禁止日志模块提供修改日志记录的能力；  3、日志如果允许删除，删除权限须控制在管理员或者系统。 |
| 10 | 防止非法监听 | 防止非法监听 | 1、提供物料所涉及到的采集、拦截最终用户原始通信内容（包括语音类、短信/彩信类、传真类、数据业务类）的功能列表，并说明涉及的通信内容类型、应用场景、存储和传输方法、保护机制。  2、在正常业务流程（建立通信连接及计费）和标准协议之外，禁止提供采集最终用户原始通信内容（语音类、短信/彩信类、传真类、数据业务类）的功能，即使出于保障网络运营和服务目的。 |
| 11 | *其它类别* | *其它安全需求* | *根据产品业务安全需要定制的，可以归类到上述分类的需求，请在相应的分类中补充，不能归类到上述分类的其它需求，如帐户管理、认证管理等，可以增加类别，在此处补充。* |