

应用软件安全检查列表

第 2.1.4 版

2004 年 6 月 25 日



国防信息系统局
现场安全操作规程

UNCLASSIFIED

目录

目录 2

1. 概述	错误!未定义书签。
1.1 审查的范围	错误!未定义书签。
1.2 审查前的准备工作	错误!未定义书签。
1.3 “安全防范审查”所需设备	错误!未定义书签。
1.4 记录结果	错误!未定义书签。
1.5 严重性代号	错误!未定义书签。
1.6 检查列表的结构	错误!未定义书签。
2. 安全防范审查报告	错误!未定义书签。
2.1 审查员信息	错误!未定义书签。
2.2 受审查单位 / 机构信息	错误!未定义书签。
2.3 应用软件信息	错误!未定义书签。
2.4 服务器综述	错误!未定义书签。
3. 检查列表说明	错误!未定义书签。
3.1 识别与认证 (I&A)	错误!未定义书签。
APP0120: 应用程序没有启用 PKI	错误!未定义书签。
APP0125: 应用程序使用非国防部 PKI	错误!未定义书签。
APP0130: 应用程序接受无效证书	错误!未定义书签。
APP0140: 应用程序用户或客户机认证进程不充分	错误!未定义书签。
APP0160: 应用程序没有启用应用客户机来认证与之通信的应用服务器	错误!未定义书签。
3.2 用户帐号管理	错误!未定义书签。
APP0210: 应用程序的用户 ID 不是唯一的	错误!未定义书签。
APP0220: 非活动用户 ID 没有被禁用	错误!未定义书签。
APP0230: 无必要的内置用户 ID 没有被禁用	错误!未定义书签。
APP0240: 用户 ID 使用了默认或弱口令	错误!未定义书签。
3.3 数据保护	错误!未定义书签。
APP0310: 敏感应用数据在静止状态时没有得到充分保护	错误!未定义书签。
APP0320: 敏感应用数据在传输过程中没有得到充分保护	错误!未定义书签。
APP0330: 应用程序使用了未经批准的加密模块	错误!未定义书签。
3.4 审计	错误!未定义书签。
APP0410: 应用程序没有充分记录安全事件	错误!未定义书签。
APP0420: 审计记录将满时应用程序没有向管理员报警	错误!未定义书签。
APP0430: 应用审计记录面对未经授权删除、改动或泄露十分脆弱	错误!未定义书签。
3.5 应用操作	错误!未定义书签。

- APP0510: 基于访问控制的应用角色没有实行职责分离..... 错误!未定义书签。
- APP0515: 应用实行动之前没有授权..... 错误!未定义书签。
- APP0520: 应用进程拥有的权限超出了正常运行的必要..... 错误!未定义书签。
- APP0530: 应用程序没有设定会话限制..... 错误!未定义书签。
- APP0550: 应用程序没有配备保密指南..... 错误!未定义书签。
- APP0560: 应用程序没有给屏幕显示和打印结果作出恰当保密标记..... 错误!未定义书签。
- APP0570: 应用程序修改应用范围以外的数据文件..... 错误!未定义书签。
- APP0580: 应用程序用户可通过意向用户界面访问支持性基础设施中的资源. 错误!未定义书签。
- 3.6 生产性应用程序的配置..... 错误!未定义书签。
- APP0610: 应用程序和支持目录包含操作期间无需调用的代码..... 错误!未定义书签。
- APP0620: 应用代码和应用数据被混杂在一起..... 错误!未定义书签。
- APP0630: 应用环境使用不必要的服务或软件..... 错误!未定义书签。
- 3.7 飞地的效果..... 错误!未定义书签。
- APP0710: 应用网络结构体系不恰当暴露飞地内资源..... 错误!未定义书签。
- APP0730: 应用程序使用未经 NIAP 批准或没有申请 NIAP 批准的 IA 或 IA 启用产品..... 错误!未定义书签。
- APP0740: 没有为应用程序制定灾难恢复计划..... 错误!未定义书签。
- APP0750: 备份或备份规程不完备..... 错误!未定义书签。
- APP0760: 没有规程确保将应用日志文件保存一年..... 错误!未定义书签。
- APP0770: 从生产数据库输出的敏感数据输入到开发数据库后未作任何改动. 错误!未定义书签。
- 3.8 应用程序的配置和授权..... 错误!未定义书签。
- APP0810: 应用程序在用户登录时没有显示适当的警告信息..... 错误!未定义书签。
- APP0820: 应用程序在会话结束后将认证证书保存在客户计算机上..... 错误!未定义书签。
- APP0830: 无特权用户可以执行特权功能..... 错误!未定义书签。
- APP0840: 应用程序用户无法明确终止会话（退出会话）..... 错误!未定义书签。
- APP0850: 认证证书或敏感信息保存在代码中..... 错误!未定义书签。
- APP0870: 应用程序包含了无效网络资源引用（路径名、URL 等）..... 错误!未定义书签。
- 3.9 移动代码..... 错误!未定义书签。
- APP0910: 应用程序发送的电子邮件信息含可执行代码..... 错误!未定义书签。
- APP0920: 应用程序传送未签名的第 1 或第 2 类移动代码..... 错误!未定义书签。
- APP0930: 应用程序传送试图访问本地操作系统资源或试图与非应用服务器的其他服务器建立网络连接的移动代码..... 错误!未定义书签。
- APP0940: 应用程序执行未经要求和验证数字签名便执行移动代码..... 错误!未定义书签。
- APP0950: 应用程序使用了某种未被现行政策涵盖的移动代码..... 错误!未定义书签。
- 3.10 基于代码的元素..... 错误!未定义书签。
- APP1010: 应用进程在停止运行前没有从内存或硬盘删除临时对象..... 错误!未定义书签。

APP1020: 应用程序在处理用户输入前没有对其进行充分验证..... **错误!未定义书签。**

APP1030: 应用程序对缓冲溢出非常脆弱..... **错误!未定义书签。**

APP1040: 应用程序不含明确的错误和例外处理能力。显示给用户的应用错误和例外提示泄露了日后会被用来发起攻击的信息..... **错误!未定义书签。**

APP1050: 应用程序故障导致出现不安全状态..... **错误!未定义书签。**

A 附录 A: 新版改动说明 **错误!未定义书签。**

附录 B: 缩略语 **错误!未定义书签。**