ICS
CCS 点击此处添加 CCS 号

T/CCIASC

中 国 计 算 机 行 业 协 会 团 体 标 准

T/CCIASC XXXX—XXXX

移动互联网应用程序（App）产品安全漏洞审核规范

Security vulnerability audit specification for mobile internet application (App) products

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国计算机行业协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件起草单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京梆梆安全科技有限公司、北京众安天下科技有限公司、哈尔滨工业大学、北京智游网安科技有限公司。

本文件主要起草人：王琦、秦晓磊、代航旅、申津津、李雪、韩继登、林魏。

移动互联网应用程序（App）产品安全漏洞审核规范

1 范围

本文件给出了移动互联网应用程序（App）产品的漏洞审核内容，提出了规范化的审核方法。

本文件适用于漏洞提交者和影响组织发现和修补漏洞，以及审核人员开展App产品漏洞审核工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 4754—2017 国民经济行业分类

GB/T 25069 信息安全技术 术语

GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 42884—2023 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南

T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写与分发要求

3 术语和定义

GB/T 4754—2017、GB/T 25069、GB/T 28458—2020、GB/T 30276—2020、GB/T 30279—2020和GB/T 42884—2023界定的以及下列术语和定义适用于本文件。

3.1

移动互联网应用程序 mobile internet application

运行在移动智能终端上的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序，简称App

注：[来源：GB/T 42884—2023，3.2]

3.2

小程序 mini program

基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

注：应用程序通过公开其应用程序编程接口（API）或函数，使外部的程序可以增加该应用程序的功能或使用该应用程序的资源，而不需要更改该应用程序的源代码

注：[来源：GB/T 41391—2022，3.3]

3.3

App提供者 mobile internet application provider

提供App产品和服务的个人或组织。

注：[来源：GB/T 30276—2020，3.2，有修改]

3.4

用户 user

使用App产品和服务的个人或组织。

注：[来源：GB/T 30276—2020，3.1，有修改]

3.5

漏洞发现 vulnerability discovery

通过技术手段，识别出网络产品和服务存在漏洞的过程。

注：[来源：GB/T 30276—2020，3.6]

3.6

漏洞提交者 vulnerability provider

从事App产品安全漏洞发现、提交等活动的组织或者个人。

注：[来源：GB/T 28458—2020，5.3.5,有修改]

3.7

影响组织 affected organization

被漏洞影响的App提供者。

注：影响组织也称受漏洞影响组织、受影响组织、漏洞影响组织。

注：[来源：GB/T 30276—2020，3.2，有修改]

3.8

漏洞管理平台 vulnerability management platform

对App产品安全漏洞进行生命周期管理的平台。

3.9

原创漏洞 original vulnerability

原创漏洞指漏洞提交者发现的漏洞，非原创漏洞指已通过公开渠道发布的漏洞。

4 缩略语

下列缩略语适用于本文件：

Payload：有效载荷

Exp：漏洞利用，Exploit

PoC：概念验证，Proof of Concept

5 漏洞审核内容与方法

5.1 漏洞资料审核

5.1.1 审核内容

审核员应对漏洞资料进行完整性、真实性与归属关系的核查，包括以下内容：

a) 漏洞提交者信息：
   1) 提交者名称；
   2) 提交者类型（个人研究者、安全研究机构、App 产品提供者、第三方平台等）；
   3) 提交者有效联系方式（电话和邮箱）；
   4) 是否原创漏洞提交（首次发现并未在其他公开渠道发布披露）；
   5) 是否自身产品漏洞（即提交者为 App 产品提供者）；
   6) 漏洞归属信息，影响组织归属漏洞提交者还是 App 产品提供者，即 App 产品提供者报送自身产品漏洞，非第三方组织提交 App 产品漏洞；
   7) 其他相关信息，是否存在高危操作需要协助等。
b) 影响组织信息：
   1) 影响组织全称；
   2) 漏洞 App 产品名称；
   3) 漏洞 App 产品版本；
   4) 影响产品类型（软件、系统）；
   5) App 产品简介与主要功能说明；
   6) 产品上架应用商店；
   7) 影响组织所属省份；
   8) App 下载量证明；
   9) 其他信息。
c) 漏洞测试环境：

1） 测试软硬件环境（品牌、型号、操作系统及版本，用于复现环境还原）；
2） App 包名（App Bundle ID 或 App Package Name），用于区别不同 App 的唯一标标识；
3） 存在漏洞的 App 产品样本（安装包文件或可下载链接）。

5.1.2 审核过程

审核员应执行以下步骤：

a） 核实漏洞提交者信息及影响组织信息的准确性；
b） 验证漏洞提交者信息的完整、真实及可联系；
c） 判断“自身漏洞”字段是否准确：
1） 若字段为“是”，需确认“漏洞提交者”与“影响组织”字段是否一致；
2） 若字段为“否”，需确认字段标注无误；
d） 核查影响组织信息及 App 产品信息的完整与准确；
e） 依据 App 包名匹配 App 名称及影响组织，验证与上报信息的一致性；
f） 验证样本文件的真实性与可用性：
1） 文件是否可正常安装运行；
2） 版本号是否与《漏洞详情》中描述一致；
g） 若未上传样本，需确认漏洞版本 App 是否可在主流应用商店公开下载；
h） 若《漏洞详情》中明确提及包含复现视频，需核实是否已上传漏洞复现视频。

5.1.3 审核结果

审核结果分为以下两类：

a） 通过：若 5.1.2 所有条款均审核通过，进入漏洞详情审核阶段；
b） 待补充资料：若 5.1.2 中部分条款审核未通过，则审核驳回，漏洞提交者重新上传相关材料。

5.2 漏洞详情审核

5.2.1 审核内容

审核员参考 T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写与分发要求，按照以下内容对《漏洞详情》进行审核：

a） 漏洞标题：简洁明确，体现漏洞类型与受影响组件（如“某公司 XXX App v3.2.1 版本存在 SQL 注入漏洞”）；
b） 漏洞类型
1） 产品型漏洞（App 产品自身缺陷）；
2） 系统型漏洞（操作系统或中间件漏洞）；
3） 第三方 SDK 漏洞；
c） 漏洞成因类别，漏洞形成的原因；
d） 漏洞描述，简述漏洞原理、触发条件及潜在危害；
e） 漏洞验证信息：
1） 完整复现步骤（含前置条件、漏洞位置、操作流程、结果证明等）；
2） 测试脚本或工具（Payload、Exp、PoC 等）；
3） 修补建议（临时缓解措施与长期修复方向）；
f） 漏洞危害等级评定（由漏洞提交者根据漏洞的影响范围、利用难度、危害程度等判定）；
g） 漏洞查重：
1） 同一组织/产品版本的重复提交漏洞查重；
2） 已收录漏洞查重；
h） 其他漏洞编号（如其他漏洞库收录已分配的漏洞编号）；
i） 漏洞复现视频（可选但推荐）：展示漏洞触发全过程，含界面操作与数据输出。

5.2.2 审核过程

审核员应执行以下步骤：

a） 查重验证：
1） 若存在相同成因且已审核通过的漏洞，终止本次漏洞；
2） 若存在未审核的同类漏洞，按提交时间优先原则处理；
b） 可利用性验证：
1） 复现步骤是否清晰可执行，现有成果是否足以证明漏洞可被利用；
2） 测试脚本是否能在指定环境中成功触发漏洞；
3） 自动化扫描工具生成报告，需进一步验证漏洞可利用性；
c） 技术一致性核验：
1） 漏洞描述与《漏洞详情》复现过程是否逻辑自洽；
2） 危害等级评估是否合理；
d） 漏洞评分：审核员根据漏洞评分标准、漏洞成因类型、危害等级及影响范围对审核通过的漏洞给予综合评分。

5.2.3 审核结果

审核结果分为以下三类：
a） 通过：技术内容完整、可验证，5.2.2 所有条款均审核通过，进入 App 产品安全漏洞认定阶段，
b） 待补充资料：若 5.2.2 部分条款审核未通过，驳回审核并要求漏洞提交者补充漏洞相关材料；
c） 不通过：若存在重复漏洞、无法复现验证漏洞或无危害漏洞，则应终止审核。

注1：漏洞评分标准：
- 低危，0.1-3.9；
- 中危，4.0-6.9；
- 高危，7.0-8.9；
- 超危，9.0-10.0。

注2：漏洞审核意见：通过的漏洞，可填写审核意见；待补充资料或不通过的漏洞，应填写审核意见。
注3：审核员需对漏洞提交信息不准确的信息进行修正。

5.3 漏洞修补方案审核

5.3.1 审核内容

《漏洞修补方案》是漏洞修复的技术蓝图，应体现修复策略的科学性与可行性。审核员应参考 T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写与分发要求，按照以下内容对《漏洞修补方案》进行审核：

5.3.1.1 修补方案通用框架（共性要求）

表1 修补方案通用框架（共性要求）

要素	内容说明
1. 漏洞基本信息	漏洞产品名称、漏洞类型、危害等级、影响版本
2. 修补目标	明确修复范围（如修复哪个接口、哪部分代码和哪个第三方组件等）
3. 修补策略	可从代码层、配置层、依赖更新、架构调整等方面描述的修复方式
4. 实施步骤	分阶段说明开发、测试、发布计划
5. 时间进度表	明确开发完成、测试验证、全量上线时间节点
6. 用户和上下游通知方案	是否推送更新提醒、是否发布安全公告
7. 回滚预案	若修复引发兼容性问题的应对措施

5.3.1.2 个性补充项（可选）

针对特殊场景可增加：多平台兼容性说明；安全加固方案；第三方SDK协调情况（如依赖库未修复时的临时方案）。

5.3.2 审核过程

审核员应执行以下步骤：

a） 核对《漏洞修补方案》与 5.2 节《漏洞详情》的技术一致性；

b） 评估修补策略的合理性：

1） 应明确漏洞影响的 App 版本及影响范围，

2） 应明确漏洞风险和漏洞修补方式；

c） 验证漏洞整改计划及时间进度安排可行性，避免“无限期延期”；

d） 确认用户和上下游产品组件及厂商告知机制已建立；

e） 将审核结果应同步至影响组织。

5.3.3 审核结果

审核结果分为以下两类：

a） 通过：若 5.3.2 所有条款均审核通过，进入漏洞修补报告审核阶段；

b） 不通过：若 5.3.2 部分条款审核未通过，影响组织根据审核员反馈意见补充相关材料。

5.4 漏洞修补报告审核

5.4.1 审核内容

《漏洞修补报告》是修复过程的技术闭环证明。审核员应参照T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写与分发要求，按照以下内容对《漏洞修补报告》进行审核：

5.4.1.1 修补报告通用结构（共性要求）

表2 修补报告通用结构（共性要求）

模块	技术要求
1. 修补过程记录	图文并茂展示代码修改、配置变更、依赖升级等操作
2. 测试验证结果	提供修复前后对比截图、自动化测试报告、渗透测试结果
3. 版本发布信息	修补后版本号、上架应用商店、发布时间
4. 安装包哈希值	提供安装文件的哈希值，确保完整性
5. 补丁说明	若为热补丁，需说明补丁范围与加载机制
6. 验证结论	明确“漏洞已修复”或“缓解措施有效”

5.4.1.2 异常情况说明（个性补充）

a） 若无法完全修复：说明技术限制、替代方案及长期规划；

b） 若仅缓解风险：说明当前控制措施的有效性与监控机制；

c） 若延迟修复：提供阶段性进展与预计完成时间。

5.4.2 审核过程

审核员应执行以下步骤：

a） 核对修补报告与漏洞详情（5.2 节）和漏洞修补方案（5.3 节）三者对应性；

b） 核查修补报告是否详细描述修补措施，需图文结合说明修复过程；

c） 若存在异常情况，需详细说明原因及计划完成时间。

d） 将审核结果应同步至影响组织。

5.4.3 审核结果

审核结果分为以下两类：

a） 通过：若 5.4.2 所有条款均审核通过，则《漏洞修补报告》符合审核要求，漏洞审核工作结束；

b） 不通过：若 5.4.2 部分条款审核未通过，则影响组织可根据审核人员反馈的意见补充相关材料。

5.5 漏洞申诉研判（漏洞专家验证）

5.5.1 审核内容

针对影响组织申诉“不认可漏洞存在”或“已修复”漏洞专家验证由技术专家对影响组织的漏洞申诉结果进行技术复审，主要包括：

a） App 类型，影响组织补充的 App 所属类型（工具类、社交类、金融类等）；

b） 影响组织所属行业，参考 GB/T 4754—2017《国民经济行业分类》；

c） 重新评估的危害等级，影响组织结合自身业务和复现核验综合评估的漏洞危害等级；

d） 评估结果，影响组织复现核验的详细过程及不认定漏洞的详细理由；

e） 漏洞详情（5.2 节）原始材料。

5.5.2 审核过程

漏洞技术专家应执行以下步骤：

漏洞技术专家复审验证过程参考5.2.2节的漏洞详情审核过程对漏洞进行复现，并对影响组织的评估结果进行审核。

5.5.3 审核结果

审核结果分为以下两类：

a） 通过：复审验证确认漏洞存在，影响组织须在限期内提交《漏洞修补方案》和《漏洞修补报告》；

b） 不通过：复审验证确认无漏洞或产品存在其他有效的安全措施，漏洞审核工作结束，归档记录。

参 考 文 献

[1] 工业和信息化部.工业和信息化部办公厅关于印发《网络产品安全漏洞管理规定》的通知（工信部联网安〔2021〕66号）[Z].2021-07-13.