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）产品安全漏洞文档编写与分发要求

Audit guide for mobile internet application (App) product security vulnerability document preparation and distribution requirements

（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：蚂蚁科技集团股份有限公司、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、董帅克、王文硕、刘子非、孙新昕、曾嘉豪、韩继登、沈晓斌。

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

1 范围

本文件给出了《漏洞详情》、《漏洞修补方案》、《漏洞修补报告》等漏洞文档的编写和分发要求，有助于安全规范地处理App产品漏洞。

本文件适用于移动互联网应用程序（App）产品提供者规范地从事App产品漏洞收集、修补和通知工作，以及漏洞提交者规范地提交《漏洞详情》。

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 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

3 术语和定义

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 internet application provider

提供App产品和服务的组织。

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。

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 漏洞文档编写要求

5.1 漏洞详情编写要求

《漏洞详情》应满足以下要求：

a) 应包括受影响 App 产品信息、影响组织信息、漏洞信息，完整详细的漏洞验证或利用过程，测试脚本（Payload、Exp、PoC）、漏洞修补建议；

b) 宜包括漏洞复现视频，演示如何利用漏洞；

c) 详情内容需客观、真实地反应漏洞的危害。

5.2 漏洞修补方案编写要求

《漏洞修补方案》应包括以下内容：

a) 漏洞分析内容，对验证后的漏洞进行简要介绍，明确漏洞位置、技术特点、原因及危害，并随附存在漏洞的代码、逻辑分析等验证材料；
b) 漏洞影响范围，至少应包括可能存在 App 产品安全漏洞的产品名称、型号、受影响的版本及用户数等影响情况；
c) 计划修补措施，描述计划修补措施。若确需较长时间修补漏洞，应给出详细理由、计划及进度安排，并告知可能受影响的用户。

5.3 漏洞修补报告编写要求

《漏洞修补报告》应包括以下内容：

a） 漏洞修补内容，对验证后的漏洞进行详细介绍，明确漏洞位置、技术特点、原因及危害，并随附存在漏洞的代码、逻辑分析等验证材料；
b） 漏洞代码来源，需描述存在漏洞代码属于自研代码，还是第三方组织代码；如果属于第三方组织代码，随附第三方组织相关信息以及是否漏洞是否修补等信息；
c） 漏洞影响范围，至少包括实际存在 App 产品安全漏洞的产品名称、型号、版本及人数等影响情况；
d） 实际修补措施，描述实际修补措施，并随附修补补丁、代码等详细材料；实际告知 App 产品用户（含下游厂商）采取软件、固件升级等措施的建议，进一步描述如何将 App 产品安全漏洞风险及修补方式告知可能受影响的用户，并提供必要的技术支持；
e） 修补状态，包括修补漏洞后的 App 版本，上架的应用商店，是否完成修补，已有多少用户完成修补，有多少用户未完成修补，未完成修补的原因、下一步计划及何时完成修补等内容。
f） 其他，针对该漏洞其他需要说明的内容。

6 漏洞文档分发基本要求

6.1 平台准入机制

漏洞文档中的报告详情应仅在漏洞管理平台内部分发传递，漏洞审核人员、漏洞提交者和影响组织必须在漏洞管理平台实名注册认证审核通过之后，方可登录平台，上传、接收或查看相关信息。

6.2 文档存储要求

a) 漏洞文档应加密存储于平台专用存储区，采用符合国家密码管理局标准的安全密码算法。
b) 漏洞元数据与内容分离存储，元数据包含漏洞编号、影响范围摘要等非敏感信息。

7 漏洞文档分发控制要求

7.1 访问权限

7.1.1 漏洞详情文档角色权限表

表1 漏洞详情文档角色权限表

角色 / 权限	漏洞提交者	影响组织	审核员	审核单位	技术专家
上传	上传	上传	\	\	\

下载	下载	下载	\	\	\
内容查看	仅自己	仅本组织	全部	全部	关联文档

7.1.2 漏洞修补方案文档角色权限表

表2 漏洞修补方案文档角色权限表

角色 权限	漏洞提交者	影响组织	审核员	审核单位	技术专家
上传	\	上传	\	\	\
下载	\	下载	\	\	\
内容查看	\	仅本组织	全部	全部	关联文档

7.1.3 漏洞修补报告文档角色权限表

表3 漏洞修补报告文档角色权限表

角色 权限	漏洞提交者	影响组织	审核员	审核单位	技术专家
上传	\	上传	\	\	\
下载	\	下载	\	\	\
内容查看	\	仅本组织	全部	全部	关联文档

7.2 传输安全

文档分发应采用安全加密通道，禁止通过邮件、即时通讯工具等外部方式明文传输。

8 操作流程

8.1 文档提交流程

漏洞提交者通过漏洞管理平台加密表单上传漏洞文档。系统自动生成唯一漏洞编号，触发审核通知机制，分配至相应审核人员。

9 安全审计

9.1 日志记录要求

完整记录以下漏洞管理平台的操作日志和运行日志，可包括不限于：文档上传/下载时间戳、用户IP地址及设备指纹、文档访问时长及操作类型。

注册记录、登录记录、漏洞操作记录、第三方接入记录、信息发布记录、用户审核记录、系统设置记录、接口调用记录。

9.2 日志保存期限

日志保存期限不少于3年。

附 录 A
（资料性）
漏洞详情编写示例

漏洞详情 (模板)

一、受影响产品名称:

受漏洞影响组织名称+APP产品名+存在漏洞APP版本号+产品平台（安卓/IOS/xxx小程序/鸿蒙/等）

二、网络产品提供者/影响企业的所属省份

三、APP 包名（APK 包名或 IPA 的 AppID 或小程序的 AppID）：XXXXXX

四、APP 哈希值：SHA256：XXXXXX

五、漏洞成因类型: XXXXXX 漏洞

六、发布情况: 未公开/公开

七、危害等级: 超/高/中/低危

八、总下载量: xxx,xxx,xxx

九、漏洞简介

尽可能详细描述：攻击者利用漏洞方式，可能执行恶意行为，造成影响结果。

十、漏洞复现

提供详细的漏洞验证过程，并附上截图。以图文的形式描述漏洞复现步骤，明确指出漏洞位置，以及如何触发漏洞的过程。必要时对复现操作步骤、原理解释和对截图添加截图的解释说明。截图需要包含时间戳信息。

图1 XXXXXX

图2 XXXXXX

图3 XXXXXX

十一、验证工具及版本

十二、验证脚本（Payload、EXP、PoC）

十三、修补建议

（注：本模板需根据具体行业特点和组织架构调整实施细节）

附 录 B
（资料性）
漏洞修补方案编写示例

漏洞修补方案（模板）

修补方案内容应至少包括：

一、漏洞分析

对验证后的漏洞进行简要介绍，明确漏洞位置、技术特点、原因及危害，并随附存在漏洞的代码、逻辑分析等验证材料。

二、漏洞影响

至少包括存在网络产品安全漏洞的产品名称、型号、受影响的版本（安卓、IOS的哪些版本）及人数等。

三、修复措施

描述修复方案，并随附修复补丁、代码等详细材料。其中，若确需较长时间修补的，请给出详细理由、计划及进度安排。

如果需要产品用户（含下游厂商）采取软件、固件升级等措施的，进一步描述是如何将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供了哪些必要的技术支持。若确需较长时间告知并支持用户修改的，请给出详细理由、计划及进度安排。

（注：本模板需根据具体行业特点和组织架构调整实施细节）

附 录 C
（资料性）
漏洞修补报告编写示例

漏洞修补报告（模板）

修补报告内容应至少包括：

一、漏洞分析

对验证后的漏洞进行简要介绍，明确漏洞位置、技术特点、原因及危害，并随附存在漏洞的代码、逻辑分析等验证材料。

二、漏洞影响

至少包括存在网络产品安全漏洞的产品名称、型号、版本（安卓、IOS的哪些版本）及人数等。

三、修复措施

描述修复方案，并随附修复补丁、代码等详细材料。

如果需要产品用户（含下游厂商）采取软件、固件升级等措施的，进一步描述是如何将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供了哪些必要的技术支持。

四、修复状态

是否完成修复，若未完成，已有多少用户完成修复，未完成修复的原因、下一步计划及何时完成修复等内容。

五、其他

针对该漏洞其他需要说明的内容。

（注：本模板需根据具体行业特点和组织架构调整实施细节）

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.