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）产品安全漏洞审核流程规范

Audit guide for mobile internet application (App) product security vulnerability audit process specification

（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、阚志刚、方宁、杨蔚、王柯龙、韩继登、刘定恒。

移动互联网应用程序（App）产品安全漏洞审核流程规范

1 范围

本文件给出了移动互联网应用程序(App)产品漏洞管理和处置中的漏洞审核生命周期的流程要求。

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

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 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和分发要求

T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞审核人员能力要求

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。

[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。

[来源：GB/T 41391—2023，3.3]

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

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]

3.5

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。

3.6

审核单位 audit enterprise

漏洞管理平台批准可以开展漏洞审核工作的单位或组织。

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 漏洞审核流程

5.1 概述

App产品安全漏洞审核工作流程包括10个部分：漏洞信息报送、漏洞资料审核、漏洞详情审核、漏洞通知、App产品安全漏洞认定、漏洞修补方案提交、漏洞修补方案审核、漏洞修补报告提交、漏洞修补报告审核、漏洞申诉研判（漏洞专家验证）。App产品安全漏洞审核流程见图1。

App产品安全漏洞审核工作流程中涉及5类角色，包括漏洞提交者、影响组织、审核员、审核单位、技术专家。不同角色在漏洞审核流程中分工见附录表1。

a) 漏洞提交者，是指 App 提供者，以及从事 App 产品安全漏洞发现、收集、通知等活动的组织或者个人；
b) 影响组织，即受漏洞影响的 App 提供者，指可能被漏洞直接或间接影响的 App 提供者；
c) 审核员，是指对上报材料（例如漏洞资料、《漏洞详情》、《漏洞修补方案》和《漏洞修补报告》等）进行审核的人，审核员来自审核单位；
d) 审核单位，是指漏洞管理平台批准的、可以开展漏洞审核工作的支撑单位；
e) 技术专家，是指漏洞管理平台的专家库里的具备漏洞相关专业知识、具备漏洞原理分析研判，具备漏洞验证能力的人。

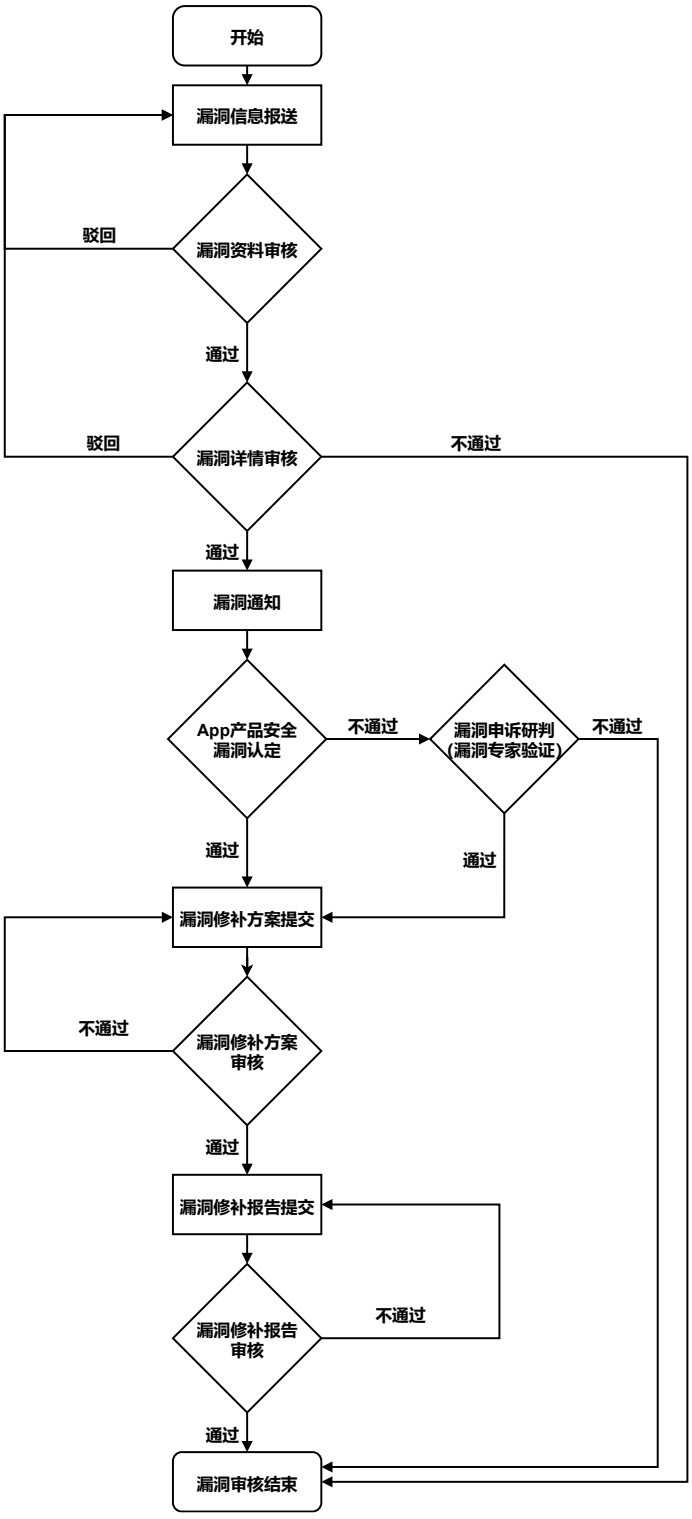

图 1 App 产品安全漏洞审核流程

5.2 漏洞信息报送

漏洞提交者向漏洞管理平台提交漏洞资料和《漏洞详情》，上报其发现的漏洞信息。

a） 漏洞资料是漏洞提交者在平台上填写的内容，应包含：漏洞提交者信息、影响组织信息、受影响 App 产品信息、漏洞信息、高危操作是否需要协助等；

b） 《漏洞详情》应包含：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）等。《漏洞详情》应按照 T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写和分发要求的要求进行编写；

c） 漏洞提交者应协助漏洞审核员对漏洞进行复现核验。

5.3 漏洞资料审核

审核员对漏洞提交者上报的漏洞资料进行审核，初步评估材料的完整性、准确性和真实性。

5.4 漏洞详情审核

审核员应依据《漏洞详情》中描述的漏洞复现过程进行审核，重点审查以下内容：

a）提交材料的准确性与完整性；

b）漏洞复现过程描述的清晰性与充分性；

c）漏洞可验证性的证实情况，确保审核员能够依照所列步骤成功复现漏洞。

在审核过程中，若审核员对漏洞存在或相关情况存有疑问，应与漏洞提交者进行充分沟通，核实相关信息。

漏洞复现失败且经核实确认漏洞不存在，漏洞审核终止。

5.5 漏洞通知

漏洞详情审核通过后，漏洞管理平台向影响组织发送漏洞通知，督促影响组织修补漏洞，降低漏洞影响危害和损失。

5.6 App 产品安全漏洞认定

影响组织在收到漏洞通知后，应在漏洞库管理平台内查看漏洞详细信息，并依据《漏洞详情》对漏洞进行复现核验、确认漏洞、评估危害等级。针对漏洞认可的情况提供原因说明。

5.7 漏洞修补方案提交

漏洞认定为通过或者漏洞申诉研判（漏洞专家验证）通过后，影响组织应编制《漏洞修补方案》，并向漏洞管理平台上报《漏洞修补方案》。《漏洞修补方案》应按照T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写和分发要求的要求进行编写。

a） 《漏洞修补方案》应包含对漏洞的预计整改计划和预期整改时间；

b） 影响组织提交《漏洞修补方案》时，应补充、修正或者更新企业信息（企业名称、行业类型、属地等）和受影响 App 产品信息（App 名称、版本等）；

5.8 漏洞修补方案审核

审核员对《漏洞修补方案》进行审核，验证漏洞分析、漏洞影响和修补措施等内容是否清晰、规范和有效。

5.9 漏洞修补报告提交

影响组织在漏洞修补方案提交审核的同时对漏洞开展修补工作。在漏洞修补完成之后，编制《漏洞修补报告》，并向漏洞管理平台上报《漏洞修补报告》。《漏洞修补报告》应按照 T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞文档编写和分发要求的要求进行编写。

a） 《漏洞修补报告》应对漏洞修补细节进行详细的图文说明；

b） 《漏洞修补报告》应包含漏洞分析、漏洞影响、修补措施和修补状态等；

c） 《漏洞修补报告》应提供补丁信息，系统型漏洞应提交系统补丁信息，App 产品型漏洞应提交修补更新的 App 补丁信息；

d） 漏洞修补报告应按照《网络产品安全漏洞管理规定》及时组织对 App 产品安全漏洞进行修补，对于需要产品用户（含下游厂商）采取软件、固件升级等措施的，应当及时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，并提供必要的技术支持；

5.10 漏洞修补报告审核

审核员对《漏洞修补报告》进行审核，验证漏洞分析和漏洞影响的合理性，以及修补措施和修补状态的有效性。

5.11 漏洞申诉研判（漏洞专家验证）

影响组织在漏洞认定不通过后，漏洞管理平台应组织技术专家进行漏洞专家验证（漏洞申诉研判）验证研判，参与漏洞专家验证的技术专家应结合企业提交的不认定原因说明，并依据《漏洞详情》对漏洞进行复现核验。

在审核过程中，若技术专家对漏洞的存在或相关情况存有疑问，应与漏洞提交者和审核员进行充分沟通，核实相关信息。

技术专家应满足T/CCIASC XXXX 移动互联网应用程序（App）产品安全漏洞审核人员能力要求的技术专家的能力要求。掌握App安全知识、计算机操作系统方面的知识、信息安全知识、网络和数据安全知识；从事信息安全、网络安全、数据安全领域的具有一定年限（3年）的工作经验，或者具有相关专业领域背景，或经过一段时间App漏洞安全专业知识技能的培训获得移动互联网安全工程师能力证书资质等。

附 录 A
（资料性）
漏洞审核流程及角色分工表

表A.1针对图1 App产品安全漏洞审核流程，给出了不同角色在漏洞审核流程中分工。

表A.1 漏洞审核流程及角色分工表

角色 / 流程	漏洞提交者	影响组织	审核员	审核单位	技术专家
漏洞信息报送	漏洞信息报送			组织审核员审核漏洞，对审核员进行培训	
漏洞资料审核	协助漏洞详情审核		审核漏洞资料信息		
漏洞详情审核	协助漏洞详情审核		审核漏洞详情信息		
漏洞通知		接收漏洞通知		通知影响组织存在漏洞，督促修补漏洞	
App产品安全漏洞认定	配合影响组织明确漏洞位置和危害	复验确认漏洞实情，修正漏洞资料信息			接收影响组织申诉漏洞
漏洞修补方案提交		修补漏洞，提交漏洞修补方案			
漏洞修补方案审核	协助漏洞修补	修补漏洞	审核修补方案		
漏洞修补报告提交		修补漏洞，提交漏洞修补报告			
漏洞修补报告审核	协助漏洞修补审核	修补漏洞	审核修补报告		
漏洞专家验证（漏洞申诉研判）	配合漏洞研判	配合漏洞研判	配合漏洞研判	组织专家对漏洞进行研判	复测并研判漏洞

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.