ICS 33.040.40
CCS L67

YD

中华人民共和国通信行业标准

YD/T 3228—XXXX
代替 YD/T 3228-2017

移动应用软件安全评估方法

Evaluation methods for mobile application security

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　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。

本文件代替YD/T 3228-2017 《移动应用软件安全评估方法》，与YD/T 3228-2017相比，除结构调整和编辑性改动外，主要技术变化如下：

检测要求发生变更如下：

a) 删除了范围中“移动智能终端预置应用软件”；
b) 在用户数据收集部分，增加了“生物特征”数据（见6.2.4.11）；
c) 增加了“用户敏感信息显示”评估（见6.3.1.7）；
d) 增加了“欺骗、误导用户授权敏感权限”的评估（见6.4.1.3.8）；
e) 增加了个人敏感信息的缓存评估（见6.4.1.7.3）；
f) 增加了动态加载第三方文件安全性评估（见6.4.1.9.2）；
g) 增加了日志安全评估（见6.4.1.10）；
h) 增加了防截屏攻击评估（见6.5.1.8）；
i) 增加了反ROOT运行评估（见6.6.1.3）；
j) 增加了利用ROOT权限调用用户敏感信息的评估（见6.6.4.2）；
k) 删除了个人信息（多媒体数据）的使用或存储的加密（见 2017版 6.）

检测方法或描述方式发生变更如下：

a) 更改了移动应用软件的术语和定义（见 3.1）；
b) 增加了“GNSS”的缩略语（见3.2）；
c) 在评估方法中增加了“不适用”的判定结果（见6.1）；
d) 在 “通讯录信息调用”部分更改“电话簿”为“通讯录”（见6.2.4.7）；
e) 更改了安装位置要求的评估步骤（见6.3.1.1）；
f) 更改了“其他应用的敏感信息收集机制”评估步骤的表述方式（见6.3.2.1.2）；
g) 更改了组件安全部分的评估步骤（见6.4.1.5）；
h) 更改了“推送消息配置的可修改功能”评估步骤的表述方式（见6.4.1.6.2）；
i) 更改了系统数据调用评估部分的评估步骤（见6.4.3.1）；
j) 更改了反编译防护部分的评估步骤（见6.5.1.1）；
k) 更改了服务器证书验证部分的评估步骤（见6.5.1.7）；
l) 更改了身份认证机制部分的评估步骤（见6.5.3.1）；
m) 更改了个人信息存储加密部分的评估步骤（见6.6.1.1.1）；
n) 更改了反模拟器运行部分的评估步骤（见6.6.1.2）；
o) 更改了密码安全评估的评估步骤（见6.6.3.3）；
p) 更改了源代码数据安全的评估步骤（见6.6.4.1）。

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这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、北京字节跳动科技有限公司、高通无线通信技术(中国)有限公司、郑州信大捷安信息技术股份有限公司、北京奇虎科技有限公司、中兴通讯股份有限公司、武汉安天信息技术有限责任公司、华为终端有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司。