讯飞安全响应中心

平台评分和奖励标准

编写人	讯飞安全响应中心
版本号	3.0
更新日期	2022.3.3

平台介绍

讯飞安全响应中心（https://security.iflytek.com/）是用于提交科大讯飞相关漏洞及威胁情报，保障科大讯飞用户（以下简称“用户”）信息安全，加强与业内同仁合作、交流的平台。

如果您对本流程有任何建议，欢迎通过邮箱（security@iflytek.com）或者官方微信（@讯飞安全，微信号：iflyteksec）的方式向我们反馈。

适用范围

本规范是用于处理讯飞安全响应中心（https://security.iflytek.com/）所收到的指定测试范围的相关安全漏洞及情报。具体测试范围请见平台官网公文。

实施日期

本规范自 2022 年 3 月 3 日起正式实施。

一、 基本原则

（1） 科大讯飞非常重视自身产品和业务的安全问题，我们承诺，每一位报告者反馈的问题都会有专人进行跟进、分析和处理，并及时给予答复或公告。

（2） 我们支持合作式的漏洞披露和处理过程，并承诺对于每位恪守“白帽子精神”，保护用户利益，帮助讯飞提升安全质量的白帽子，我们会给予感谢与回馈。

（3） 我们严禁一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞入侵业务系统、窃取用户数据、恶意传播漏洞、暗藏木马后门及不完整上报等。

（4） 我们认为每个安全漏洞的处理和整个安全行业的进步，都离不开业界各方的共同合作。希望企业、安全公司、安全组织和安全研究者一起加入到“合作式的漏洞披露”过程中来，一起为建设安全健康的网络环境而努力。

二、 漏洞/情报反馈与处理流程

（1） 预报告阶段：漏洞报告者前往讯飞安全响应中心（https://security.iflytek.com/）（以下统称“指定平台”）建立帐号。

（2） 报告阶段：报告者登录指定平台，提交相关信息。

（3） 处理阶段：一个工作日内，工作人员会确认收到的报告并跟进开始评估问题，五个工作日内工作人员处理问题、给出结论并计分，特殊情况可能会有延期。必要时与报告者沟通确认，请报告者予以协助。

（4） 修复阶段：针对安全漏洞，业务部门修复漏洞并安排更新上线，修复时间根据问题点严重程度及修复难度而定。客户端漏洞受版本发布限制，修复时间根据实际情况确定。针对情报，由于情报分析调查的时间较长，因此确认周期相比漏洞的时长较长，具体时间需根据实际情况确定。

（5） 完成阶段：完成处理后，报告者可通过积分在科大讯飞安全响应中心平台兑换礼品。

三、 安全漏洞评分标准

3.1 计分规则

危害等级：依据严重、高危、中危、低危、无影响（忽略）五个等级进行判断。

系数说明：根据讯飞产品的影响程度和发展现状，我们将在评分标准接收范围内的产品划分高、中、低三个系数。具体明细清单可见平台公告。讯飞安全团队将根据业务开展实际情况，进行相应调整。

3.2 Web/APP 漏洞危害等级

得分结果参考					
		严重	高危	中危	低危
系数	高	400~600	200~350	80~180	5~50
	中	300~400	120~280	30~80	2~20
	低	200~300	100~180	10~60	1~2

【严重】

1. 直接获取核心系统权限的漏洞，包括但不限于任意代码执行、任意命令执行、上传 Webshell 并可执行等。
2. 直接导致核心业务大量数据泄露的漏洞，包括但不限于核心数据库的 SQL 注入漏洞。
3. 核心业务的严重业务逻辑缺陷。包括但不限于任意账号密码重置、任意账号登录等。

【高危】

1. 直接获取重要业务系统权限的漏洞，包括但不限于任意代码执行、任意命令执行、上传 Webshell 并可执行等。
2. 直接导致重要业务大量数据泄露或者核心业务部分数据泄露的漏洞，包括但不限于重要或部分核心业务数据库的 SQL 注入漏洞。
3. 重要业务的严重业务逻辑缺陷。包括但不限于任意账号密码重置、任意账号登录、越权操作等。
4. 可远程获取客户端系统权限的漏洞。包括但不限于：远程命令执行、远程代码执行等。

【中危】

1. 可直接获取一般业务系统权限的漏洞，包括但不限于 webshell 上传、远程命令执行、文件包含等。
2. 一般系统的敏感信息泄露，包括但不限于普通系统 SQL 注入漏洞、线上服务器账户密码等。
3. 任意文件上传导致的重要或核心系统的存储 XSS、JSONP 劫持等漏洞。
4. 普通的逻辑设计缺陷和流程缺陷，包括但不限于非核心的业务规则绕过。

【低危】

1. 要用户多次交互或者强交互才可触发的漏洞。包括但不限于无法构成较大危害的存储 XSS 等。
2. 利用场景有限的漏洞。例如：URL 跳转。
3. 只能造成轻微影响的其他漏洞。

【忽略】

1. 无法利用或者利用价值极小的漏洞。包括但不限于 self-xss、无意义的反射 XSS、csrf、无实际影响的 slowhttptest 等、无敏感信息的 jsonp 劫持、GitHub 内网 IP、邮箱泄漏、phpinfo 泄露、短信轰炸等。
2. 无法利用或无危害的“漏洞”，包含但不限于 SSRF 漏洞，只是简单的访问 DNSlog，无明显影响。
3. 不能重现的漏洞，包括但不限于和漏洞审核员反复沟通均无法重现的漏洞。
4. 移动端：无意义的打印。
5. 内部已知漏洞，包括但不限于已在通用平台上公开的漏洞、内部安全人员已经发现的漏洞。
6. Redis、Zookeeper 等未授权并且无实际或者极少量业务数据的漏洞。
7. 不能直接体现漏洞的其他问题，包括但不仅限于纯属用户猜测的问题、不包含

敏感信息的测试页面等。

8. 非测试范围内的漏洞。
9. 其他讯飞认为可以忽略的漏洞。

3.3 智能硬件漏洞危害等级

得分结果参考（硬件）					
		严重	高危	中危	低危
系数	高	800~1000	400~700	100~300	10~80
	中	400~600	200~350	80~180	5~50
	低	300~400	120~280	30~80	2~20

【严重】

1. 互联网环境下的无交互远程命令执行。
2. 互联网环境下的因严重的漏洞导致较大的经济损失。

【高危】

1. 可获取大量用户敏感信息。
2. 非互联网环境下的远程命令执行漏洞。

【中危】

1. 需要强交互的命令执行漏洞。
2. 非重要功能模块的逻辑漏洞。

【低危】

1. 少量的信息泄露。
2. 需要强交互或者物理接触的安全风险漏洞。
3. 强交互的拒绝服务漏洞。

3.3 影响范围说明

【大】涉及核心业务，且对大量敏感数据、资金等有极大影响。

【中】涉及一般业务，或对业务产生一般影响。

【小】涉及边缘业务，或对业务系统影响有限。

四、 安全情报评分标准

得分结果参考（安全情报）				
威胁系数 / 情报完整性	严重（26~40）	高危（9~25）	中危（3~8）	低危（1~2）
最完整（10）	260~400	90~250	30~80	10~20
~	~	~	~	~
最不完整（1）	26~40	9~25	3~8	1~2

4.1 安全情报威胁系数

【严重】

1. 针对核心业务系统的完整入侵证据或漏洞线索，如核心生产服务器被上传 webshell 等。
2. 大量核心业务数据库被流传贩卖。
3. 对核心业务有重大直接影响的黑灰产情报。

【高危】

1. 针对非核心业务系统的完整入侵证据或漏洞线索，能够帮助讯飞安全响应中心对入侵事件溯源分析、定位攻击者身份等。
2. 对核心业务有较大直接影响的黑灰产情报。

【中危】

1. 对特定产品服务造成一定影响的黑灰产详细情报。
2. 能够帮助完善防御体系的详细情报以防御高风险及以上级别危害的新型攻击方式、技术等。

【低危】

1. 未对用户造成实际影响，但经过确认对业务有一定影响的情报。
2. 黑灰产组织相关信息。

【忽略】

1. 少量用户信息泄露。
2. 无法追溯问题根源，不能证实的威胁情报。
3. 对业务用户影响不大，在可承受范围内。
4. 由于情报的时效性，报告已知或已失效的情报不计分。

4.2 情报完整性说明

由于情报的完整性对情报的价值有着重要的影响，因此上报情报的价值会进行情报完整性考量。情报完整性的评价会综合情报的多个方面进行考虑。讯飞安全响应中心会根据提供情报的完整度给出 0-10 分的评定，仅上报单一方面的情报将不计分。情报线索关键点包括：

（1）攻击者个人或者组织的信息，比如身份信息、联系方式、交流渠道等。
（2）攻击者的场景信息，比如产品或业务入口，页面地址等。
（3）攻击过程还原。

【无效情报】

无效威胁情报是指：错误、无意义或根据提供信息无法调查利用的威胁情报，例如：

（1）上报虚假捏造或者无法还原的情报信息。
（2）只上报可能存在情报的聊天群，但未提供其他有效信息。
（3）上报已过期、已失效的威胁情报。

五、 评分标准补充说明

（1） 在未获得讯飞 SRC 的许可下即使漏洞已经修复完成也不要将漏洞的相关信

息向任何的第三方透露或者公开。

（2） 针对通用型漏洞，以官方发布漏洞通告时间为准，存在一个月的锁定时间，在锁定时间内，我们会安排业务自查、修复。锁定时间结束后可正常提交并按照《讯飞安全响应中心评分奖励标准》正常评分。特殊情况以平台单独公告为准。

（3） 同一漏洞源产生的多个漏洞，漏洞数量为一个，同一应用组件导致的漏洞最多只记为三个。例如同一业务系统的同类组件漏洞、同一接口不同参数导致的 SQL 注入漏洞、PHPwind 的安全漏洞、同一个 JS 引起的多个安全漏洞、同一个发布系统引起的多个页面的安全漏洞、框架导致的整站的安全漏洞、泛域名解析产生的多个安全漏洞、同一个 URL 多个参数的相同问题、多个站点使用相同的接口引起的漏洞、同一个站点多个目录存在目录浏览或 SVN/Git 信息泄露、同一个站点开启 Debug 等原因引起的多处信息泄露等。

（4） 通用型的组件漏洞，例如 Fastjson 反序列化、Weblogic 反序列化等仅给前三个提交的漏洞进行计分，其他的同样漏洞均不再计分。

（5） 以安全测试为借口，利用漏洞进行损害用户利益、影响业务正常运作、私自公开、盗取用户数据等行为的，将不会计分，已支付的有权收回，同时讯飞安全响应中心将保留采取进一步法律行动的权利。

（6） 同一份报告中提交多个漏洞，只按危害级别最高的漏洞计分。

（7） 无实际危害证明的扫描器结果，不计分。

（8） 同一漏洞/情报被重复提交的，讯飞安全响应中心将以最先提交且清晰表达、重现此问题的报告者为唯一奖励者。

（9） 各等级漏洞/情报的最终得分由危害大小、利用难易程度及影响范围综合因素决定，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的 XSS 漏洞，则可跨等级调整漏洞分值。

（10） 测试过程中，仅需证明漏洞存在即可，不要做进一步利用，若因进一步的渗透行为导致的任何事件讯飞安全响应中心将保留采取进一步法律行动的权利。

（11） 人为自行制造安全威胁或安全事件情报的不计分，同时讯飞安全响应中心将保留采取进一步法律行动的权利。

（12） 对于 RCE、SQL 注入、XSS、越权等漏洞的测试，请遵循“测试程度最小化”的原则，仅证明漏洞存在即可，不要进行过度测试。例如 RCE 漏洞，仅 curl dnslog 地址即可，不要进行反弹 shell 操作。

（13） 任何情况下不要通过任何安全漏洞拖取讯飞及其分子公司资产下的任何数据。

（14） 不允许进行任何 DoS 或者 DDOS 攻击。

六、 季度奖励标准

名次	奖励	封顶
第一名	奖励额度=本季度积分*1 +证书	800 分

第二名	奖励额度=本季度积分*0.5 +证书	400 分
第三名	奖励额度=本季度积分*0.2 +证书	200 分

6.1 季度奖励说明

（1） 奖励以积分形式，直接加入平台账户中，可进行正常礼品兑换。

（2） 计算周期：以季度（3 个月）为周期，评选截止时间为每个季度最后一天。

（3） 证书寄送：获奖人需在结果公布 10 日内，将“收货地址+平台个人页面截图”发送至 security@iflytek.com ，以便证书顺利寄送。

（4） 本奖励自 2022 年 1 月 1 日起开始实施。

七、 奖励发放原则

（1） 常规奖励：奖品使用积分兑换，1积分≈10RMB。

（2） 非现金礼品将于10个工作日内发放，如兑换者未能及时完善个人信息导致礼品不能按时发放的，将延迟发放；如因礼品兑换者个人过失、快递公司问题及人力不可抗拒因素导致的奖品损坏及/或丢失，讯飞安全响应中心不承担责任。

（3） 现金礼品兑换，请参考平台《现金兑换须知》公告。

（4） 特殊奖励：讯飞安全响应中心将不定期举行特殊活动，发放对应活动奖励。对于价值较高的漏洞/情报，我们将发放额外奖励。

（5） 特别提醒： 对于讯飞及关联公司的从业人员，请至内部平台反馈报告。提交自己所负责业务的安全问题不予奖励。

八、 争议解决办法

在漏洞/情报处理过程中，如果报告者对处理流程、评分等有异议的，可通过以下方式联系讯飞安全响应中心工作人员：

（1） 讯飞安全响应中心（https://security.iflytek.com/）平台安全报告的详情页留言板留言。

（2） 邮箱：security@iflytek.com 。

（3） 微信公众号（@讯飞安全，微信号：iflyteksec）留言。

讯飞安全响应中心将按照报告者利益优先的原则处理，必要时会引入外部安全人士共同裁定。