Soul 安全应急响应中心漏洞处理和评分标准

文档修订记录	V1.02021-08-11 发布第一版
版本	V1.0
日期	2021-08-11

适用范围

本标准适用于 SOUL 安全应急响应中心“SoulSRC”

https://security.soulapp.cn/）所收到的所有情报。

实施日期：本标准自 2021 年 10 月 10 日起施行。

基本原则

1）SOUL 非常重视自身产品和业务的安全问题，我们承诺，对每一位 SoulSRC 平台用户反馈的问题都有专人进行跟进、分析和处理，并及时给予答复。

2）SOUL 在处理 SoulSRC 平台用户反馈的问题时可能需要用户提供必要的帮助，譬如，为了有效地处理及跟进问题，SOUL 可能需要报告者协助一同复现问题。SOUL 反对和谴责在提交反馈报告后一切遮掩漏洞细节或抗拒协助的消极行为。对于提交 SOUL 认可的高质量报告并在报告、反馈和积极响应跟进等过程中提供有效帮助的 SoulSRC 平台用户，SOUL 也会酌情给予相应的奖励。

3）SOUL 鼓励并支持负责任的漏洞披露并且协助 SOUL 处理漏洞的 SoulSRC 平台用户，我们承诺，对于每位恪守“白帽子”精神，保护用户利益，帮助 SOUL 提升安全质量的 SoulSRC 平台用户，我们将给予感谢和合理的回馈。

4）SOUL 反对和谴责一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益和 SOUL 平台利益的黑客行为，包括但不限于利用漏洞盗取用户隐私及虚拟财产、入侵业务系统、窃取用户数据、恶意传播漏洞等。

5）SOUL 反对和谴责一切利用安全漏洞恐吓用户、攻击 SOUL 平台系统或竞争对手的行为。

6）SOUL 认为每个安全漏洞的处理和整个网络安全行业的进步，都离不开各方的共同合作。希望企业、安全公司、安全组织、安全研究者一起加入到“负责任的漏洞披露”过程中来，一起为建设安全健康的互联网环境而努力。

评分标准通用原则

1）评分标准仅针对对 SOUL 产品和业务有负面影响的威胁情报。SOUL 产品和业务，系指域名包括但不限于*.soulapp.cn 的服务器（包括 SOUL 运营的服务器），产品为 SOUL 发布的各类客户端产品。经 SOUL 判定对 SOUL 业务安全无负面影响的威胁情报，不计分。

2）通用型漏洞（即由同一个漏洞源产生的多个漏洞）仅计为一个漏洞数量。例如同一个 JS 引起的多个 XSS 漏洞、同一个发布系统引起的多个页面的 XSS 漏洞、框架导致的整站 XSS/CSRF 漏洞、泛域名解析产生的多个 XSS 漏洞、同一域名下同一组件产生的多个 flashxss 漏洞等。

3）对于第三方库（比如 libpng、zlib、libjpeg 等）导致的客户端漏洞（包括 PC 端和移动端），且可以通过升级或者更换第三方库可完成修复的漏洞，仅给首个漏洞报告者计分。

4）对于移动终端系统导致的通用型漏洞，比如 webkit 的 uxss、代码执行等，仅给首个漏洞报告者计分，对于其它产品的同个漏洞报告，均不再另外计分。

5）由于客户端漏洞审核本身比较复杂并且涉及到其它的开发部门，审核时间可能较 WEB 漏洞长，有时可能由于报告者提供的漏洞细节不够详尽，导致 SoulSRC 无法按约定时间内给出结论，请各位用户理解。为了加快 SoulSRC 审核及弥补安全漏洞，请各位用户在反馈漏洞时提供完整的 poc/exploit 与验证视频，并提供相应的漏洞分析。烦请知悉，如果未提供完整的 poc/exploit 与验证视频，或者没有详细分析的漏洞，将可能直接影响评分。

6）如果同一时间周期内提交同一客户端的多个漏洞，请用户在反馈漏洞时明确给出导致漏洞和触发漏洞的关键代码,以便 SoulSRC 快速确认是否为相同漏洞，加快漏洞确认时间。

7）对于第三方通用型漏洞导致的安全问题，依据通用漏洞奖励标准。

8）提交威胁情报的用户在复查安全问题时，如果发现其此前反馈的安全问题在 SoulSRC 处理完成之后仍然存在或未完全修复好，则用户据此重新提交反馈报告的，当作新威胁情报继续计分。

9）同一条威胁情报，第一个报告者得分，其他报告者不得分；提交网上已公开的威胁情报不计分。

10）拒绝无实际危害证明的扫器结果。

11）以安全测试为借口，利用情报信息进行损害用户利益、影响业务正常运作、修复前公开、盗取用户数据或其他违法违规侵害 SOUL 及其他第三方合法权益等行为的，将不会计分，同时 SOUL 保留采取进一步法律行动的权利。

12）禁止未经 SOUL 事前书面授权，私自公开漏洞的行为，一旦发现严肃处理，包括奖励取消、SoulSRC 平台账户禁用等。

13）在法律允许的最大范围内，本标准所有内容最终解释权归 SoulSRC 所有。

漏洞/威胁情报反馈与处理流程

[预报告阶段]

情报报告者在按照指示注册之后即认为同意接受 Soul 安全应急响应中心的授权（https://security.soulapp.cn/index.php/report）生成帐号。

[报告阶段]

SoulSRC 平台用户登陆 Soul 安全应急响应中心，提单反馈威胁情报（报告状态将显示为：待审核）。

[处理阶段]

1）自 SoulSRC 平台用户成功提交威胁情报后的一个工作日内， SoulSRC 工作人员会确认收到的威胁情报报告并跟进开始评估问题（报告状态将显示为：审核中）。

2）自 SoulSRC 平台用户成功提交威胁情报后的三个工作日内，SoulSRC 工作人员处理问题、给出结论并计分（报告状态将显示为：已确认/已忽略）。必要时工作人员会与 SoulSRC 平台用户沟通确认，请用户届时予以必要协助。

[修复阶段]

1）SOUL 业务部门修复威胁情报中反馈的安全问题并安排更新上线（报告状态将显示为：已修复）。修复时间根据问题的严重程度及修复难度而定，一般来说，

严重和高风险问题 24 小时内，中风险 3 个工作日内，低风险 7 个工作日内。客户端安全问题受版本发布限制，修复时间根据实际情况确定。

2）威胁情报的报告者复查安全问题是否修复（报告状态将显示为：已复查/复查异议）。

[完成阶段]

1）SoulSRC 每自然月的第一周内，发布上月威胁情报处理公告，向上月的威胁情报报告者致谢并公布威胁情报处理情况。

2）威胁情报报告者可以使用积分值在积分商城兑换现金或实物礼品，兑换完成后，SoulSRC 会根据兑换的结果相应地为威胁情报报告者发出现金或礼品；同时，SoulSRC 也会视实际情况不定期地提供奖励及线下活动。

3）在得到威胁情报报告者许可的情况下，SoulSRC 将不定期挑选有代表意义的威胁情报进行分析，分析文章将发表在 SoulSRC 官网。

漏洞/威胁情报评分标准

SOUL 威胁情报主要包含三大部分的内容：业务漏洞、安全情报、通用软件漏洞。根据目前 SOUL 产品的重要程度和发展现状，我们将在漏洞赏金范围内的产品划分为核心产品、普通产品、边缘产品，（对三种产品类型对判定，解释权归 SoulSRC 所有）下面我们将分别描述范围和评分标准。

核心产品范围描述

目前在漏洞奖励计划中的“核心产品”范围仅包含以下可能影响 SOUL 绝大多数用户的核心产品功能（列表会持续更新）：

1. Soulapp 核心功能

2. Soulapp 海外版 核心功能

普通产品范围描述

*.soulapp.cn、soul ip 资产 内部资产 数据信息等存在安全漏洞

边缘产品范围描述

对业务影响较少的，边缘域名下的漏洞

SoulSRC 安全币体系基于以上的产品范围描述，SoulSRC 针对不同产品范围的安全报告构建起 SoulSRC 安全币体系，并根据该体系作为主要参考为符合条件的 SoulSRC 平台用户提供奖励。计算公式：单个漏洞安全币=积分*贡献系数，具体的贡献系数由 SoulSRC 根据实际情况进行认定。举例说明：依据该体系，当 SoulSRC 平台用户提供一个核心产品(见上述核心产品范围述)的严重漏洞并获得 SoulSRC 平台最终确认时，该用户将可能获得至少 9*60=540 的安全币奖励。具体情况详见下表：

SoulSRC 安全币体系				
危害等级	积分	贡献系数		
		边缘	普通	核心
低	1-2	2	4	8
中	3-5	2	6	10
高	6-8	8	10	30
严重	9-10	10	30	60

1 个安全币价值人民币 10 元，所以对应的现金奖励范围如下：

SoulSRC 安全币体系				
危害等级	积分	折算现金奖励（人民币元）		
		边缘	普通	核心
低	1-2	20-40	40-80	80-160
中	3-5	60-100	180-300	300-500
高	6-8	480-640	600-800	1800-2400
严重	9-10	900-1000	2700-3000	5400-6000

漏洞报告质量奖

我们鼓励 SoulSRC 平台用户提供更加清晰、定位明确且能帮助业务快速跟进的漏洞报告，并为高质量报告者提供最高等值于 1000 元人民币的安全币。当 SoulSRC 平台用户为其发现的安全问题编写并提供优质报告时，该名用户就有

机会在漏洞经 SoulSRC 确认后直接获得前述的安全币。SoulSRC 将根据优质报告的实际情况，为不同的报告分配相应额度的漏洞报告质量奖。

例如：漏洞利用链复杂或需多账号多动作才可以达成利用效果的漏洞，逐步编写漏洞利用流程，并为每个动作提供如 HTTP 请求包文本、测试思路、详细的 Payload、可一键执行并复现的 POC 脚本或已尝试的 Payload 列表和日志等信息，帮助 SoulSRC 和业务同事快速准确地复现、跟进和修复漏洞，满足以上情况的报告将有机会获得漏洞报告质量奖。

严重漏洞额外现金奖

对于为核心业务或重点业务提供高质量严重漏洞报告的用户，SoulSRC 将额外提供现金奖励，按季度进行发放。奖励标准如下：

核心产品的严重漏洞：最高为税后人民币 5000 元上限

年度特别奖励

根据 SoulSRC 平台用户提交报告的严重/高危漏洞数量、报告内容详实、协助复现与修复、保持友好沟通、遵守安全测试规范、对收敛类似风险的帮助、对优化安全系统的帮助等多方面进行综合评选年度特别奖励获得者。年度奖励内容根据实际活动由 SoulSRC 进行制定。

业务漏洞评分标准

根据漏洞危害程度分为严重、高、中、低、无五个等级，每个等级评分如下：

严重：

1、直接获取核心系统权限（服务器端权限、主打产品客户端权限）的漏洞。包括但不仅限于：远程任意命令执行、上传获取 WebShell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。

2、严重的逻辑设计缺陷。包括但不仅限于任意帐号登录、任意帐号密码密保修改、任意帐号资金消费。

3、严重的敏感信息泄露。包括但不仅限于重要 DB 的 SQL 注入、包含敏感信息的源文件压缩包泄露。

4、直接导致核心业务拒绝服务的漏洞。包括但不仅限于直接导致线上业务拒绝服务、可导致大量客户端用户崩溃掉线等（DDoS 攻击等资源耗费型的拒绝服务除外）。

高危：

1、重要敏感信息泄露。包括但不仅限于 SQL 注入、可获取任意信息的 XXE 漏洞、系统层面的任意路径遍历。

2、核心业务未授权访问。包括但不仅限于绕过认证直接访问线上环境的管理后台、后台弱口令等。

3、敏感越权操作。包括但不仅限于越权修改其他客户端用户帐号重要信息、越权操作订单等。

4、核心业务且大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的存储型 XSS（包括存储型 DOM-XSS）、可自动传播的 CSRF 等。

中危：

1、普通的存储型 XSS，涉及核心业务敏感操作的 CSRF、反射型 XSS 等。

2、普通信息泄露。包括但不仅限于客户端密码明文存储、包含敏感信息的源代码压缩包泄露。

3、普通越权操作、逻辑设计缺陷和流程缺陷。如核心业务应用未授权访问。

低危：

1、轻微信息泄露。包括但不仅限于单独的危害较低的 Web 层的路径遍历、目录浏览、信息泄露如路径信息泄露、svn 信息泄露、phpinfo 等。

2、URL 跳转。包括但不仅限于未验证的重定向和转发。

3、客户端本地拒绝服务漏洞。包括但不仅限于组件参数未验证导致的拒绝服务漏洞。

4、利用困难仅造成轻微影响的漏洞。包括但不仅限于反射型 XSS（包括反射型 DOM-XSS、FlashXSS）、低版本浏览器下的 XSS（老旧版本忽略处理）、CRLF、普通操作的 CSRF。

无：

1、无实际危害的问题。包括但不仅限于产品功能缺陷、页面乱码、样式混乱、不泄露敏感信息的报错。

2、不能重现的漏洞。包括但不仅限于经 SoulSRC 工作人员确认无法重现的漏洞。

3、无法利用或者没有利用价值的漏洞。包括但不仅限于无意义的目录遍历、401 基础认证钓鱼、有编码缺陷但无法利用的问题、Self-XSS、无敏感操作的 CSRF、无意义的异常信息泄露、无实际危害证明的扫描器结果、无敏感信息的 jsonhijacking、仅有 js 与 img 等的打包文件、一般信息的 logcat 等。

4、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。

5、SSRF 漏洞无法获取内网的相关服务器信息，只是简单的访问 dnslog，无任何影响。

6、非核心客户端本地拒绝服务漏洞。包括但不仅限于组件参数未验证导致的拒绝服务漏洞。

7、Zookeeper、memcache、redis、普通的运维管理系统等未授权访问，没有数据或者其他可利用的地方，可以忽略。

安全情报评分标准

安全情报是指 SOUL 的产品和业务漏洞相关的情报，包括但不限于漏洞线索、攻击线索、攻击者相关信息、攻击方式、攻击技术等。

情报报告必须经过情报提供者的验证和复现并提供相关证明材料（不限于复现截图和视频）用于证明威胁情报真实有效；情报提供者需写清事实依据，同时应该

反馈详细复现信息包括但不限于复现行为开始时间，复现行为结束时间，复现结果和结果证明，复现账号和 ID 等。

根据危害及情报提供情况详细评分标准如下表：

评分级别	线索范围	描述
严重	服务器被入侵且提供了入侵行为方式等相关线索	业务服务器被入侵且提供了相关行为 特征方便快速定位确认问题点
	核心业务敏感数据泄露线索	业务数据库被拖取，且提供了数据库详细信息，方便快速定位确认问题点
	重大金融逻辑漏洞线索	支付类严重的逻辑漏洞

高	蠕虫传播且提供了蠕虫传播的链 接等相关线索	核心业务存储型 XSS 导致的大规模蠕虫传播
	用户身份信息大规模被窃取且提供了攻击代码等相关线索	因漏洞引起的大规模身份信息被窃取
	核心产品外挂线索	核心产品可严重影响产品功能平衡的 外挂线索
中	能够帮助完善防御系统以防御高风险及以上级别危害的新型攻击方式、技术等	新型 WebShell、DDoS 等攻击方式

奖励发放原则

[常规奖励]

礼品需要 SoulSRC 用户使用其通过 SoulSRC 平台合法获得的安全币予以兑换，安全币数量由威胁情报的评分乘以相应危害等级系数而得，危害等级系数参考“漏洞/威胁情报评分标准”章节（该系数会由 SoulSRC 根据实际情况调整，每次调整会公告发布）。多个威胁情报产生的安全币可累加，除非特别声明，未使用的安全币不会过期。

礼品上架时有数量限制，当期上架奖品被兑换完后不再接受兑换，先到先得。

礼品每月邮寄两次，15 号之前兑换的当月中下旬邮寄，15 号之后兑换的次月月初邮寄。如因报告者未能及时完善资料导致的延误，将顺延至下个月批量寄送时寄出；如因报告者过失、快递公司问题及不可抗力等非归因于 SoulSRC 的因素产生的奖品丢失或者损坏，SoulSRC 不承担任何责任。

[季度奖励]

奖励规则：以每个自然季度为一次评选周期；

当季度提交高危及以上漏洞数量≥3 且当季度所提漏洞安全币排名前三；

奖励金额：第一名 人民币 5000 元 第二名 人民币 3000 元 第三名 人民币 1000 元；

奖金发放：按照自然季度，以现金奖励形式发放；

规则说明：如在当季度结束后未有达到规则要求的“安全专家”，当季度的奖励名额将作废。

争议解决办法

在威胁情报处理过程中，如果报告者对处理流程、威胁情报评定、威胁情报评分等具有异议的，直接发送邮件到 security@soulapp.cn 提交反馈，或联系平台工作人员微信：chirebingxue，会有工作人员及时响应。SoulSRC 将根据威胁情报报告者合法利益优先的原则进行处理，必要时可引入外部人士共同裁定。

FAQ

Q：SoulSRC 平台的 1 个安全币相当于多少人民币？

A：根据目前公示的奖励标准，当前 SoulSRC 平台 1 个安全币相当于 10 元人民币。

Q：在 Soul 安全应急响应中心上的威胁情报会公开吗？

A：为了保护用户利益，在威胁情报反馈的安全问题修复前，威胁情报相关信息均不会公开。安全问题修复后，且经 SoulSRC 书面授权后，该项威胁情报的报告者才可以公开。本着“授人以鱼不如授人以渔”的考虑，SoulSRC 建议威胁情报报告者将威胁情报相关技术进行归类和总结，以技术文章的方式公开，且不展示具体产品名称，并且不得披露任何 Soul 客户端用户相关的任何信息。

Q：SOUL 威胁情报奖励计划是不是用奖品隐瞒安全问题？

A：不是。首先，我们认为，在威胁情报中的安全问题未修复前，为了保护 Soul 客户端用户的合法利益，威胁情报不应该被公开，这也是业界的通用做法。其次，SOUL 为威胁情报报告者提供礼品等奖励是为了表达对威胁情报报告者的感谢和尊重，绝对不是用奖品隐瞒威胁情报中的安全问题。

Q：SOUL 有没有先“忽略”漏洞然后偷偷修复？

A：绝对不会。提交的“漏洞”一旦进入“忽略”状态，相关的审核人员会在评论中留下忽略的原因。常见情况可能是这个“漏洞”不被认定为是漏洞而被评估为一个“bug”，SoulSRC 会将详细情况反馈给 Soul 客户端的相关产品同事，是否更改这个“bug”由产品同事决定；另外一种可能的情况是业务本身的变动，导致“漏洞”后续不复存在。但是不论如何，SOUL 都不会“偷偷修复漏洞”。