360SRC 外部漏洞处理和评分标准

编写人	360 安全应急响应中心
版本号	V2.0
实施日期	2023 年 3 月 1 日

版本号	修订记录	发布日期
V2.0	1. 优化漏洞评分体系； 2. 优化漏洞贡献值体系、个人成长体系； 3. 优化月度、年度奖励计划； 4. 更改漏洞奖金发放方式； 5. 新增漏洞报告质量奖励； 6. 新增隐私漏洞评分细则； 7. 新增 FAQ。	2023.3.1
V1.0	发布第一版	2021.4.7

目录

360SRC 外部漏洞处理和评分标准 V2.0

(2023.03.01)

前言

为提高 360SRC 的处理效率，增进 360SRC 与白帽子的合作，我们将漏洞奖励标准进行统一，后续白帽子提交的漏洞情报等级将按照本标准进行评定。

如果您对本标准有任何的建议，可通过 360SRC 官方邮箱（security@360.cn）或者微信公众号（360 安全应急响应中心）向我们进行反馈。本标准自 2023 年 3 月 1 日起施行。

一、适用范围

本标准适用于 360 集团发布的产品和业务，此外 360 集团所投资的公司、子公司、合资公司等也在收录范围内，具体范围可参考 https://security.360.cn/Product/product。

二、威胁反馈与处理流程

1. 漏洞报告模板

漏洞报告内容需包含漏洞名称、漏洞类型、漏洞等级、漏洞详情	
【漏洞名称】	漏洞名称、影响域名
【漏洞类型】	正确的漏洞类型
【漏洞等级】	低/中/高/严重
【漏洞 URL】	URL
【漏洞详情】	详细说明：包括域名、涉及的接口、参数及应用版本等
	漏洞证明：包括利用条件、详细实现步骤，要有明确的触发位置，关键步骤和漏洞利用条件可尽量截图说明，仅从理论层面说明漏洞的存在而无利用和复现过程将不予收录。（例如扫描报告、请求头配置等）

	漏洞危害：危害是重要评级依据
	修复方案：建议在报告中描写清晰

2. 漏洞审核

在漏洞审核过程中我们可能与报告者沟通确认，请予以协助。对于 web/服务端/移动端漏洞，我们将在三个工作日内进行审核；其他漏洞审核时间可能有所延长。

3. 漏洞确认及修复

漏洞审核通过后，漏洞状态会更改为“正在修复”，业务部门将修复所报告的问题，修复时间根据问题严重程度、修复难度和业务情况而定。

Web 端、服务端、客户端的严重及高危漏洞若三个月内未修复，白帽子可以重新提交漏洞，**客户端漏洞仅收录第一次**。

4. 漏洞定级

漏洞确认后将进行初评级，初评级后**七个工作日内**我们将与业务沟通并进行漏洞最终定级**（初评级阶段不显示漏洞等级与奖励）**。

5. 安全币发放

我们在漏洞最终定级后将会把安全币发放至白帽子账户中，漏洞详情页显示安全币金额则为已发放。

6. 兑换现金

白帽子可每月 1 至 7 日在 360SRC 官网商城用安全币兑换现金，**安全币兑换数量应不低于 20 个**。兑换现金前请准确填写相关信息，包括本人姓名、身份证号码、户名、银行账号和开户行（需具体到支行），白帽子应确保信息准确无误，否则由此导致的付款延迟等由白帽子自行负责。我们将在兑换后统一发放现金，如遇有节假日或其他特殊事由，发放时间可能延迟。

三、漏洞奖励标准

1. 基础奖励标准

漏洞奖励=业务系数*基础安全币。

360SRC 根据业务的重要程度分为核心业务、一般业务、边缘业务三类。其中核心业务为 360 集团发布的价值较高、影响范围较广的业务和产品；边缘业务为日活量较低、影响范围较为有限的业务和产品；其他业务和产品归属为一般业务。

【核心业务产品】

https://security.360.cn/News/news/id/294

【业务系数】

业务系数		
核心业务	一般业务	边缘业务
1.2~1.5	0.8 ~ 1.0	0.1~0.5

漏洞奖励主要分为以下六种：Web/服务端漏洞、移动端漏洞、PC 客户端漏洞、智能硬件端漏洞、隐私安全漏洞、威胁情报、Xsafe 计划漏洞。

【Web/服务端漏洞奖励】

漏洞安全币（安全币 ： RMB=1 : 5）				
等级	严重	高危	中危	低危
基础安全币	1000 ~ 1400	300 ~ 600	30 ~ 100	2 ~ 15
核心业务（1.2 ~ 1.5）	1200 ~ 2100	360 ~ 900	36 ~ 150	3 ~ 23
一般业务（0.8 ~ 1.0）	800 ~ 1400	240 ~ 600	24 ~ 100	2 ~ 15
边缘业务（0.1 ~ 0.5）	100 ~ 700	30 ~ 300	3 ~ 50	1 ~ 8

【移动端漏洞奖励】

漏洞安全币（安全币 ： RMB=1 : 5）				
等级	严重	高危	中危	低危
基础安全币	1000 ~ 2000	600 ~ 800	200 ~ 400	5 ~ 20
核心业务（1.2 ~ 1.5）	1200 ~ 3000	720 ~ 1200	360 ~ 600	6 ~ 30

一般业务（0.8 ~ 1.0）	800 ~ 2000	480 ~ 800	160 ~ 400	4 ~ 20
边缘业务（0.1 ~ 0.5）	100 ~ 1000	60 ~ 400	20 ~ 200	1 ~ 10

【PC 客户端漏洞奖励】

漏洞安全币（安全币 ： RMB=1 : 5）				
等级	严重	高危	中危	低危
基础安全币	800 ~ 1200	200 ~ 600	100 ~ 200	5 ~ 15
核心业务（1.2 ~ 1.5）	960 ~ 1800	240 ~ 900	120 ~ 300	6 ~ 23
一般业务（0.8 ~ 1.0）	640 ~ 1200	160 ~ 600	80 ~ 200	4 ~ 15
边缘业务（0.1 ~ 0.5）	80 ~ 600	20 ~ 300	10 ~ 100	1 ~ 8

【智能硬件漏洞奖励】

漏洞安全币（安全币 ： RMB=1 : 5）				
等级	严重	高危	中危	低危
基础安全币	3000 起	1000 ~ 2500	400 ~ 800	20 ~ 300
核心业务（1.2 ~ 1.5）	3600 起	1200 ~ 3750	480 ~ 1200	24 ~ 450
一般业务（1.0）	2400 起	800 ~ 2500	320 ~ 800	16 ~ 300
边缘业务（0.1 ~ 0.5）	300 起	80 ~ 1250	40 ~ 400	2 ~ 150

【隐私漏洞奖励】

漏洞安全币（安全币 ： RMB=1 : 5）			
等级	高危	中危	低危
基础安全币	100 ~ 150	40 ~ 80	1 ~ 20
核心业务（1.2 ~ 1.5）	120 ~ 225	48 ~ 120	2 ~ 30
一般业务（0.8 ~ 1.0）	80 ~ 150	32 ~ 80	1 ~ 20
边缘业务（0.1 ~ 0.5）	10 ~ 75	4 ~ 40	1 ~ 10

【威胁情报奖励】

漏洞安全币（安全币 ： RMB=1 : 5）				
等级	严重	高危	中危	低危
基础安全币	600 ~ 1000	200 ~ 500	30 ~ 100	2 ~ 15

核心业务 （1.2～1.5）	1200～1500	360～750	36～150	3～23
一般业务 （0.8～1.0）	480～1000	160～500	24～100	2～15
边缘业务 （0.1～0.5）	60～500	20～250	3～50	1～8

【X・Safe 计划漏洞奖励】

漏洞安全币（安全币 ： RMB=1：5）				
等级	严重	高危	中危	低危
安全币	2000 起	300～1000	150～300	1～30

2. 额外奖励

点赞币奖励：若白帽子提供的漏洞报告完整、清晰、漏洞定位明确并同时能够帮助审核及业务跟进处理，则可能被认定为优质漏洞报告。360SRC 将根据优质漏洞报告内容和作用等为报告者奖励一定的点赞币。**点赞币将统一发放为安全币，1 点赞币等于 1 安全币。**

点赞币（点赞币：安全币 =1：1）		
严重	高危	中危
0～100		

举例：若白帽子提交一个核心业务、严重的 Web 漏洞报告，该漏洞报告完整、清晰、准确定位漏洞且白帽子迅速帮助业务跟进修复了漏洞，经业务认定为优质漏洞报告并奖励 20 点赞币，那么白帽子能够获得的安全币数量为：1000*1.2+20=1220 个（对应￥6100 元）。

四、漏洞贡献值

漏洞贡献值=漏洞基础贡献值*业务系数（漏洞基础贡献值=漏洞基础安全币/5）

漏洞基础贡献值				
漏洞类型	严重	高危	中危	低危
web 漏洞 基础贡献值	200～280	60～120	6～20	1～3
移动安全漏洞 基础贡献值	200～400	120～160	40～80	1～4
PC 客户端漏洞 基础贡献值	160～240	40～120	20～40	1～3
智能硬件漏洞	600 起	200～500	80～160	4～60

基础贡献值				
隐私漏洞 基础贡献值	/	20～30	8～16	1～4
威胁情报 基础贡献值	120～200	40～100	6～20	1～3

自 2023 年 3 月 1 日起，白帽子新提交的漏洞报告将以计算漏洞贡献值，之前的漏洞贡献积分也将统一替换为漏洞贡献值，替换比率为 1：1。我们将按照原有贡献值和新增贡献值总和进行排行，包括总排行、年度排行、季度排行、月度排行。

五、白帽子荣誉等级和成长等级

荣誉等级：我们将根据白帽子自注册之日起已经获得的贡献值总和评定荣誉等级，荣誉等级将于每日 24：00 进行更新。

成长等级：我们将根据白帽子上月最后一日前溯 720 日计算已经获得的贡献值总和并评定成长等级，成长等级将于当月 15 日进行更新。

荣誉等级	成长等级	旧榜单：积分	新榜单：贡献值
初窥门径	LV1	0～199	0～199
略有小成	LV2	200~799	200~799
小有名气	LV3	800~1599	800~1599
闻名遐迩	LV4	1600~2499	1600~2499
如雷贯耳	LV5	2500 及以上	2500 及以上

六、360SRC 专属福利

1. 月度个人奖励

https://security.360.cn/News/news/id/295

2. 月度团队奖励

https://security.360.cn/News/news/id/231

3. 年度个人奖励

年度个人贡献值排 TOP5 的白帽子将获得额外现金奖励、参加 360SRC 年度颁奖典礼及旅游名额。

4. 年度团队奖励

年度团队贡献值排 TOP3 的团队核心成员将获得参加 360SRC 年度颁奖典礼及旅游名额。

（原季度旅游奖励已取消，升级年度个人奖励人数。若出现不可抗力因素，颁奖典礼及旅游可能会出现延期或取消情况）

七、漏洞定级标准

漏洞主要分为以下六个内容：Web\服务端、移动端漏洞、PC 客户端漏洞、智能硬件端、隐私安全漏洞、威胁情报。

根据漏洞对业务产生的危害，分为严重、高危、中危、低危、忽略五个等级。收录的基本原则是有实际应用危害。

各类型漏洞评分标准如下：

Web\服务端

【严重】

1、直接获取核心服务器权限的漏洞，包括但不限于上传 Webshell、任意代码执行、远程命令执行等。

2、直接导致严重的信息泄露漏洞，包括但不限于重要数据库的 SQL 注入、系统权限控制不严格等导致的敏感数据泄露漏洞等。

3、直接导致严重影响的逻辑漏洞，包括但不限于核心账户体系的账密校验逻辑等。

【高危】

1、重要业务敏感数据信息泄露漏洞，包括但不限于重要用户信息、订单信息、数据文件信

息等。

2、重要业务的逻辑漏洞，包括但不限于权限绕过等。

3、不需交互的重点业务漏洞，包括但不限于文件遍历、任意文件包含、任意文件读取等。

4、包含重要业务敏感信息的非授权访问，包括但不仅限于绕过认证直接访问管理后台、后台弱密码、可直接获取大量内网敏感信息的 SSRF 等。

【中危】

1、不需交互对用户产生危害的安全漏洞，包括但不限于一般页面存储型 XSS 等。

2、普通信息泄露漏洞，包括但不限于用户信息泄露和业务敏感信息泄露等。

3、普通的逻辑设计缺陷和流程缺陷，包括但不限于越权查看非核心系统的订单信息等。

4、其他造成中度影响的漏洞，例如：没有敏感信息的 SQL 注入、无回显 SSRF 漏洞等。

【低危】

1、在特殊条件下才能获取用户信息的安全漏洞，包括但不限于反射 XSS 等。

2、轻微信息泄露，包括但不限于服务器物理路径、边缘系统文件、本地日志等。

3、其他造成低危害的漏洞，例如：管理后台开放、解析漏洞、存在可被暴力破解接口等。

【忽略】

1、无关安全的 bug。包括但不限于网页乱码、网页无法打开、某功能无法用。

2、无法利用的“漏洞”。包括但不限于没有实际危害的“扫描”报告、Self-XSS、无敏感信息的 JSONHijacking、无敏感操作的 CSRF、无意义的源码泄漏、内网 IP 地址/域名泄漏、401 基础认证钓鱼、程序路径信任问题、无敏感信息的信息泄漏（如无敏感信息的 /metrics，/.htaccess，/DS_store，/ swagger-ui 等）。

3、非 360 业务漏洞，测试系统的无效漏洞。

移动端漏洞

【注：APP 中 API 接口漏洞按照 web 漏洞奖励标准评估】

【严重】

1、远程代码执行，远程以 App 权限执行任意代码。包括但不限于具备完整利用链的内存破坏漏洞、利用动态库覆写或其它业务逻辑上问题导致的远程任意代码执行；

2、远程应用静默安装，远程或弱交互方式实现任意应用的静默安装。包括但不限于浏览器点击、扫码等方式；

3、影响范围广的逻辑漏洞，包括但不限于核心账户体系的账密校验逻辑问题导致任意用户登录。

【高危】

1、本地代码执行，本地以 App 权限执行任意代码，包括但不限于具备完整利用链的内存破坏漏洞、利用动态库覆写或其它业务逻辑上问题导致的远程任意代码执行；

2、本地提权漏洞，本地提权至 App 权限执行敏感操作、包括但不限于打开 App 任意保护组件、静默安装任意应用、修改 App 安全设置以及短信读写，客户端沙箱数据读写等漏洞；

3、核心业务敏感数据/信息泄露，包括但不限于重要用户信息、订单信息、任意文件读取等。

【中危】

1、需交互的对用户产生危害的漏洞，普通越权操作，包括但不限于可查询其它少量用户数据的越权操作，任意组件调用等漏洞；

2、本地任意文件读取，本地以 App 权限读取应用内的沙箱文件；

3、一般业务敏感数据/信息泄露，包括但不限于重要用户信息、订单信息、任意文件读取等。

4、应用破解类漏洞，包括但不限于应用内购、VIP 功能破解、账号权限绕过等漏洞。

【低危】

1、可造成实际危害的 url 跳转等风险、危害较小的安全问题；

2、远程拒绝服务漏洞，包括但不限于攻击接口、页面导致的拒绝服务、APP 远程拒绝服务等。 指定任意用户或手机号无限制的短信轰炸问题；

3、其它造成低危害的漏洞，例如：管理后台开放、解析漏洞、存在可被暴力破解接口等；

4、需要物理接触或在特定场景下需用户配合才能造成的用户信息泄漏相关漏洞。

【忽略】

1、与安全无关的 bug，包括但不限于产品功能缺陷，网页乱码、设备适配等。

2、无利用价值的问题，包括但不限于 App 反编译风险、无敏感操作的 CSRF、无意义的源码泄漏、内网 IP 地址/域名泄漏等。

3、本地拒接服务漏洞，只能通过手机本地临时造成 App 崩溃的问题。 无法影响其他用户、无法复现、危害过低的漏洞。

PC 客户端漏洞

PC 客户端产品包括 360 安全卫士、360 杀毒、360 手机卫士等核心产品，其他客户端产品视情况降低评级。长期不更新或较低版本的产品不列入奖励范畴，若危害较大可酌情给予奖励。

【严重】

包括但不限于远程任意命令执行、可利用的远程缓冲区溢出以及其它因逻辑问题导致的远程代码执行漏洞。

【高危】

主动防御绕过，即执行高危动作后未出现拦截。高危动作包括但不限于修改启动项、替换系统命令、设置定时任务、破坏或删除卫士功能、致程序崩溃防御失效的操作等。

备注：主动防御绕过需在联网且开启晶核的模式下；高危动作不包括正常文件读取、截屏等行为。

【中危】

1、本地任意代码执行。

包括但不限于本地可利用的堆栈溢出、本地提权、文件关联的 DLL 劫持以及其它逻辑问题导致的本地代码执行漏洞。

备注：不包括以下几种情况：

加载不存在的 DLL 文件、加载正常 DLL 未校验合法性、需要管理员权限操作手工拷贝 DLL、需要用户大量交互以及基于 KnownDLLs 缺陷所导致的 DLL 劫持等。

2、会影响用户正常使用场景的拒绝服务攻击。包括但不限于远程应用拒绝服务攻击、组件权限导致的本地拒绝服务漏洞等。

3、其他功能缺陷。包括但不限于客户端敏感信息明文存储传输、下载恶意文件未提示及其他类似问题。

【低危】

安全扫描的绕过，即静态免杀样本，或其他危害较低的软件缺陷。

智能硬件漏洞

智能硬件产品范围：360 路由器，360 智能摄像机，360 儿童手表，360 行车记录仪等。

【严重】

无条件远程代码执行等漏洞以及未授权远程终端控制漏洞。以路由器为例：在远端 Internet 环境下，在设备未授权状态下直接与路由器 WAN 口通信，触发漏洞并获取路由器内部系统 root 权限，实现远程代码执行。

【高危】

包括但不限于有条件的远程代码执行、无条件局域网代码执行、远程设备通用密码方案破解。例如在不知道路由器管理密码的情况下，通过利用路由器 LAN 口的漏洞取得 root 权限并执行任意代码。

【中危】

包括有条件局域网代码执行、远程拒绝服务（非耗光系统资源）、物理接触导致的设备通用密码方案破解等。

【低危】

包括局域网内拒绝服务（非耗光系统资源）、通过物理接触打断 uboot、物理调试接口开放等。

【忽略】

对于只可以使设备功能异常，或泄露一些配置文件（无隐私信息）的设备逻辑问题，只属于程序设计的 bug，不按漏洞进行奖励,对于有价值的反馈，会进行公开致谢。

隐私安全

隐私漏洞收录产品仅限如下列表 APP：360 手机卫士、360 账号卫士、360 手机助手、360 移动浏览器、360 儿童卫士、360 安全云盘、360 家庭防火墙、360 摄像机 APP、360 智慧生活、360 扫地机器人。

【高危】

1. 问题影响重大，与所在市场国家地区相关法律法规严重冲突；

2. 行业内罕见问题，发现方式新颖需要一定技术深度才能发现。

【中危】

1. 问题影响一般，未及时修复可能导致用户投诉、监管机构通报等影响；

2. 问题属于监管机构已经明确的检查项目，需要一般技术手段可发现。

【低危】

1. 问题影响小，未及时修复可能产生的影响不明确；

2. 一般情况下，该类问题不需要技术手段就可以发现。

威胁情报

威胁情报评分标准将结合实际影响、情报完整性和业务重要程度进行综合评定。具体原则如下：

1、威胁情报需包括情报具体内容、情报的数据真实性证明和情报来源等关键信息。未能主动证明真实性的情报将被忽略。各个内容是否全部包含为评分的必要条件。

2、原则上威胁情报奖励不高于对应漏洞奖励。

3、收录内容包括：服务器被入侵且提供了入侵行为特征等关键线索

4、核心业务数据库被下载，并提供数据库名或文件等关键线索；支付业务逻辑漏洞利用、业务流程绕过等关键线索；蠕虫传播、流量劫持等提供源链接、网络数据包样本等关键线索；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；对有针对性的秒杀、刷积分、活动刷钱套现等事件提供关键线索；360 相关钓鱼网站实际控制人员的信息提供关键线索；对泄露公司内部数据、用户数据等行为提供关键线索等。

5、质量评判：标题准确概括情报内容（加分）、情报内容准确详细（加分），数据证明清晰、逻辑完整（加分），原始情报来源可溯源（必要）。若缺乏可溯源，评价将在一定范围内降级。

八、漏洞审核原则

1、评分标准和漏洞奖励仅针对对 360 产品和业务有影响的漏洞。360 的产品或业务参见 https://security.360.cn/Product/product。对于不再更新的产品或未纳入安全服务的控股业务，相关漏洞将不予收录（例如鲸鱼阅读、或其他尚未列入资产的新收购产品等）。

2、同一漏洞导致的多个利用点按照级别最高的奖励执行；同一系统三个月内只收取前三个接口产生的同类型漏洞（例如同个系统的不同接口存在水平越权漏洞）。

3、同一漏洞源的多个漏洞仅记为 1 个。以下情况也作同一漏洞源处理，即多个漏洞按一个处理。例如：同一个站点开启 debug 或 php 未关闭错误回显等原因引起的多处信息泄露；同一个站点多个目录存在目录浏览或 svn 信息泄露；同一个接口的逻辑漏洞。

4、同一漏洞有多个白帽子提交漏洞报告的，将以在先提交且清晰表述并重现漏洞的白帽子为准。

5、对于有活动期限或是即将下线的业务，经审核可能会跨等级调整贡献值。

6、通过测试环境获取的数据为测试数据，或者获取到测试环境的服务器权限，按照 0.1 系数给予奖励。测试环境所获数据属于若与正式环境一致，则按照 1 倍系数给予奖励。

7、隔离网段和公有云上的业务漏洞，将视情况下调或忽略评级，定级范围最高为高危，若与业务无关则不予收录。若能证明相关漏洞影响较大，可酌情考虑按正常标准评级。

8、通用漏洞。对于 CVE 等通用漏洞，在漏洞公开的前 10 个工作日，相关的漏洞暂不予收录，若 10 个工作日后业务或资产存在对应漏洞，则可向 SRC 提交对应漏洞，依据通用漏洞奖励标准，且仅以首个漏洞提交者奖励。

9、特殊漏洞说明：

（1）弱口令漏洞与未授权登陆，若通过进入后台没有敏感信息或者敏感操作，定级范围为低危至中危。

（2）url 跳转漏洞，对于非核心业务的 url 跳转漏洞和仅能跳转到子域名的 url 跳转漏洞暂不予收录。

（3）SSRF 漏洞需能到达内网域名或 IP，仅通过外网 dnslog 证明不予认定；无回显或部分回显的 SSRF 漏洞定级范围为低危至中危。

（4）触发条件苛刻的漏洞，将视业务情况忽略或降低评级奖励。

（5）CSRF 漏洞，非核心业务的非敏感操作 CSRF 漏洞暂不予收录。

（6）由于以消耗基础设施资源并导致其崩溃或故障来完成的拒绝服务攻击暂不予收录。

（7）需要物理访问用户设备的攻击或中间人攻击暂不予收录。

（8）360 安全卫士、360 杀毒漏洞收录条件：开启晶核、联网状态、软件版本为最新版本；dll 劫持等漏洞需通过程序自动执行而非手工移动。

（9）同一漏洞的绕过或不同利用方式 360SRC 仍会进行收录，收录奖励系数为原漏洞奖励的 0.2～0.5（根据业务系数判断）。

10、未纳入安全服务的资产一般情况下不收录相关漏洞，例如 1360.com 等域名存在第三方厂商使用的资产或公有云上的资产，若证明存在重大危害且可影响 360 集团业务也会视情况收录。

九、通用规定

1、禁止将漏洞报告存放在互联网开放的云服务或共享文档中，如因此造成漏洞泄露的，对该漏洞不予奖励。

2、对提交漏洞报告后、未修复漏洞前，将漏洞报告公开或泄露的不予奖励。发现漏洞后不得私自公开，否则 360SRC 将严肃处理，包括取消奖励或采取进一步措施。

3、白帽子在进行渗透测试时，如在线上对业务做增删改操作时，不得对正常用户数据做操

作。任何以漏洞测试为借口，利用漏洞进行损害用户利益、影响业务正常运作、修复前公开、盗取用户数据等行为在溯源发现后将不予奖励，同时 360 保留采取进一步法律行动的权利。

4、在漏洞测试过程中，须遵守渗透测试原则，严格遵守《中华人民共和国网络安全法》等法律法规之规定；对于上传 webshell、反弹 shell、内网扫描探测、恶意拖取数据、下载源码等违法违规行为，360 保留对违法违规者采取进一步法律行动的权利。

5、SQL 注入测试过程中，证明危害即可，获取十条以上数据者追究更加数据情况做出相应处理；敏感数据泄露，请在漏洞修复后删除相关信息，一旦发现信息泄露，亦做出相应处理。

6、360 集团及关联方员工不参与 SRC 漏洞奖励计划，请通过内部渠道报告漏洞，一经发现将取消相关奖励。

7、白帽子如对处理流程、漏洞评定、漏洞评分有异议，可在评论区进行反馈。若仍有异议可通过 security@360.cn 邮箱申请漏洞仲裁。

8、本标准最终解释权归 360 信息安全部所有。

FAQ

Q： 360SRC 的 1 个安全币相当于多少人民币？

A： 1 个安全币=5 元人民币

Q： 新标准生效前获得的现金如何处理？

A：新标准生效前已经获得的漏洞奖金，将在审核通过且收到准确收款信息后发放至白帽子提交的银行账户中，23 年 2 月份的漏洞奖金将于 23 年 3 月中下旬发放。

Q： 新标准生效前获得的积分如何处理？

A：新标准生效前获得的积分将等额替换为安全币，即 1 积分=1 个安全币，白帽子可在官方商城用安全币兑换现金或商品。

Q：新标准生效后荣誉等级、成长等级如何计算？

A：荣誉等级为白帽子自注册之日起已经获得的贡献值总和评定荣誉等级，成长贡献值为白帽子上月最后一日前溯 720 日计算已经获得的贡献值总和并评定成长等级。

白帽子新提交的漏洞报告将以计算漏洞贡献值，之前的漏洞贡献积分也将统一替换为漏洞贡献值，替换比率为 1：1，我们将按照原有贡献值和新增贡献值总和进行计算。

Q：安全币翻倍活动期间，贡献值是否翻倍？

A：我们可能不定期举行安全币翻倍活动，活动期间白帽子提交漏洞报告且最终定级的，所获得的安全币翻倍，但贡献值不变、不翻倍。若白帽子在双倍活动期间，提交了一个核心业务价值基础安全币为 500（基础贡献值为 100）、业务系数为 1.2 的 web 高危漏洞，最终获得安全币为 500*1.2*2=1200，获得贡献值为 100*1.2=120 分。