本安全漏洞评分标准及奖励规则生效日期：2019 年 7 月 15 日

一．MFSRC 奖励计划

马蜂窝安全应急响应中心奖励计划采取贡献值兑换形式实行，白帽子通过提交有效漏洞来获得贡献值，贡献值由漏洞风险等级以及业务分级系数决定，奖励贡献值公式：

奖励贡献值=漏洞风险等级*业务分级系数*倍数奖励（默认为 1）

举例：白帽子提交一个马蜂窝有效漏洞，MFSRC 根据**漏洞风险等级**及**业务分级系数**评判，漏洞风险等级值为 15，业务分级系数为一级，并且当前在活动期，倍数奖励为 2，则奖励白帽子该漏洞的积分为：

15*200*2=6000 贡献值=6000 RMB

如果白帽子提交漏洞所涉及系统为核心应用且等级为高危以上可计算额外奖励，奖励贡献值据具体情况而定，**范围参考 2000-20000 之间。**

注：（1）活动期倍数会增加；

（2）白帽子可用获得的贡献值在积分商场里兑换礼品，每个白帽子账户中的贡献值可以累积，但仅供个人使用。

贡献值梳理表：贡献值=漏洞风险等级*业务分级系数*倍数(默认为 1)

业务分级系数*漏洞风险等级*倍数（默认为 1）	严重漏洞（16-20）	高危漏洞（11-15）	中危漏洞（6-10）	低危漏洞（1-5）
一级（200）	3200-4000	2200-3000	1200-2000	200-1000
二级（80）	1280-1600	880-1200	480-800	80-400
三级（30）	480-600	330-450	180-300	30-150
其他（10）	160-200	110-150	60-100	10-50

二．MFSRC 业务分级系数

MFSRC 业务分级系数		
业务分级	业务分级系数	举例
一级	200	交易中心
二级	80	内容中心
三级	30	边缘业务
其他	10	其他

三．MFSRC 漏洞风险等级

【 严重 16-20 】

本等级包括：

1、直接获取操作系统权限（服务端权限、客户端权限）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、缓冲区溢出、SQL 注入获取系统权限等；

2、严重的敏感信息泄漏：包括但不限于：重要 DB（资金、用户身份、订单）的 SQL 注入引起的敏感信息泄漏；绕过认证直接访问管理后台、后台弱密码、获取大量内网敏感信息；可获取大量核心用户的身份信息、订单信息、银行卡信息等接口问题引起的敏感信息泄露等；

4、严重的逻辑漏洞：包括但不仅限于涉及用户支付方面的安全问题，如任意账号登录、任意账号密码修改、任意账号资金消费、批量修改任意帐号密码漏洞等。

【 高危 11-15 】

本等级包括：

1、影响范围较广的越权访问漏洞：包括但不仅限于账号越权修改重要信息、进行订单普通操作、重要业务配置修改等较为重要的越权行为等；

2、直接获取移动客户端权限：包括但不限于任意命令执行、任意代码执行等；

3、直接导致系统业务拒绝服务的漏洞：包括但不限于直接导致业务重要接口拒绝服务漏洞；

4、高风险的信息泄露漏洞：包括但不限于 DB 的 SQL 注入漏洞，泄露用户隐私信息，服务器敏感信息的日志文件下载等；

5、大范围影响用户的其他漏洞。包括但不限于可造成自动传播的重要页面的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、资金、密码等。

【 中危 6-10】

本等级包括：

1、需交互才能获取用户身份信息的漏洞：包括但不限于敏感操作的可造成严重危害的存储型 XSS 等；

2、普通越权操作。包括但不仅限于不正确的直接对象引用、越权查看订单信息、越权查看用户身份信息等。

3、普通信息泄漏：包括但不仅限于客户端明文存储密码、系统路径遍历；

4、普通逻辑设计缺陷：包括但不限于短信验证码绕过、邮件验证绕过；

【 低危 1-5】

本等级包括：

1、轻微信息泄漏。包括但不仅限于路径信息泄漏、git 信息泄漏、SVN 信息泄漏，以及客户端应用本地 SQL 注入（仅泄漏数据库名称、字段名、cache 内容）、日志打印、配置信息、异常信息等。

2、难以利用但存在安全隐患的漏洞：包括但不仅限于难以利用的 SQL 注入点、不能引起较大危害的存储型 XSS（包括仅自己可见的存储型 XSS）等；

3、其他只能造成轻微影响的漏洞：包括但不仅限于 URL 跳转、系统/服务运维配置不当、组件权限漏洞等。

【 忽略 】

本等级包括：

1、不涉及安全问题的 BUG：包括但不限于产品功能缺陷、页面乱码、样式问题、静态文件目录遍历、应用兼容性等问题；

2、无法利用的漏洞：包括但不限于难以利用的 self-xss、非敏感操作的 CSRF、无敏感信息的 json hijacking 等

3、无敏感信息的信息泄露：包括但不限于无意义的源码泄漏、无意义的内网 IP 地址/域名/账号密码泄漏、路径信息泄露、无敏感信息的 logcat 信息泄漏等。

4、不能重现的漏洞：包括但不仅限于纯属用户猜测、未经过验证的问题、无实际危害证明的扫描器结果。

四、漏洞收集原则：

1、MFSRC 收集漏洞范围：

马蜂窝名下所有产品及业务，域名包括但不限于*.mafengwo.cn。

2、相同问题的漏洞，将按提交时间给予首个提交者积分。

3、如果同一漏洞或同一问题漏洞的不同表现形式在漏洞修复前由多位漏洞报告者提交，在进行奖励时，我们会以最先提交并清晰表述、重现此漏洞问题的研究者为唯一受奖励者。

4、漏洞提交报告应尽量详细、规范。提供详细的漏洞详情、漏洞原理、利用方式以及修复建议的可以酌情加分。漏洞需证明其存在并可利用，对于 poc 或 exploit 未提供或者没有详细分析的漏洞提交将直接影响该漏洞的评定。

5、漏洞证明其存在并可利用，禁止利用漏洞进行非法操作，包括但不限于：拖库、进入内网，情节严重者将取消该用户所有贡献值，并保留采取进一步法律行动的权利。

6、MFSRC 漏洞奖励计划仅限于首次在 MFSRC 提交的漏洞，在其它平台上提交过的，同一漏洞非首次提交的，均不予审核通过。提交网上已经公开的漏洞不计分。严禁白帽子在多平台提交相同漏洞来刷奖励，一经发现将严肃处理。

7、恶意提交者将作封号处理。

8、由于客户端的特殊性，提交漏洞以当前时间最新客户端为准(同一漏洞不可在不同版间重复提交)。

9、只接收属于马蜂窝移动客户端产品的漏洞，不接收 Android/IOS 系统自身漏洞。

10、马蜂窝坚决抵制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、盗取用户数据等恶意行为，一经发现将进行严肃处理，同时马蜂窝保留采取进一步法律行动的权利。

五、漏洞争议解决办法：

白帽子在漏洞提交及处理过程中，如果对流程处理、漏洞定级、漏洞评分等有异议的，可注明漏洞标题、漏洞提交人、漏洞提交时间、联系方式（电话/微信）、申诉原因等内容邮件至：mfsrc@mafengwo.com，MFSRC 将按照漏洞报告者利益优先的原则处理，必要时可引入外部安全人士共同裁定。