东方财富安全应急响应中心（EMSRC）

漏洞评分与奖励标准

版本号 3.0

编写人	东方财富安全应急响应中心
版本号	3.0
更新日期	2019-03-14
执行日期	2019-04-01

目 录

适用范围

东方财富安全应急响应中心，以下简称 EMSRC。本流程适用于东方财富安全应急响应中心反馈平台(http://security.eastmoney.com)、东方财富安全应急邮箱 security@eastmoney.com 、媒体平台（官方微博和微信官方公众号）所收到的所有漏洞和情报。

如果您对本流程有任何的建议，欢迎通过邮箱（security@eastmoney.com,此方式为推荐）或者微博私信（http://weibo.com/emsrc）、微信公众号互动的方式向我们反馈。

EMSRC 原则申明

东方财富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有专人进行跟进、分析和处理，并及时给予答复。

东方财富支持负责任的漏洞披露和处理过程，我们承诺，对于每位恪守“白帽子精神”，保护用户利益，帮助东方财富提升安全质量的白帽子，我们会给予感谢和回馈。

东方财富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、损害企业和用户利益的黑客行为，包括但不限于利用漏洞盗取用户隐私信息及虚拟财产、入侵业务系统、影响业务运作、窃取用户数据、恶意传播漏洞等。

东方财富反对和谴责一切利用安全漏洞恐吓用户、攻击竞争对手的行为。

东方财富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“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。

特别注意事项：需要注意的是，由于东方财富旗下东方财富证券公司股票业务的特殊性，在股市开盘当天（AM 9:00—PM 15:00），不可使用相关工具扫描，不可使用大批量并发的安全测试方法，以及 DDoS 等危害系统稳定的手段进行所谓测试。

东方财富愿与业界各安全公司、安全组织和安全研究者一起共建安全可靠的网络空间。

一、 业务漏洞反馈和处理流程

1.1 预报告阶段

东方财富安全应急响应中心漏洞反馈平台唯一网络地址：

https://security.eastmoney.com

以下简称 EMSRC。

漏洞报告者打开东方财富安全应急响应中心漏洞反馈平台，并注册账号（东方财富通行证账号）。以通信证账号登录到 EMSRC。

1.2 报告阶段

漏洞报告者登陆东方财富漏洞反馈平台，提交漏洞信息（状态：待确认）。

1.3 处理阶段

一般情况下，三个工作日内，EMSRC 工作人员处理问题，给出结论并评分（状态：确认中）。必要时会与报告者沟通确认，请报告者予以协助。

1.4 完成阶段

业务部门修复漏洞并安排更新上线（状态：已确认/已忽略）。修复时间根据问题的严重程度及业务部门修复难度而定，一般情况下，严重和高风险漏洞 72 小时内，中等风险在七个工作日内，低风险十个工作日左右会给与状态确认。客户端漏洞受版本发布限制，修复时间根据实际情况确定。确定之后 EMSRC 关闭漏洞处理流程。

二、贡献值与安全币计算方法

1、【贡献值】由漏洞对应危害程度和业务以及应用的的重要性决定：

贡献值 = 应用系数 * 基础贡献值

2、【安全币】由漏洞对应危害程度和业务以及应用的的重要性决定

安全币 = 应用系数 * 基础安全币

示例：1 个直接获取核心在线服务器权限的严重漏洞可获得 5000 RMB 奖励

贡献值 = 基础贡献值（严重：10）* 应用系数（核心：10）=100 贡献值

安全币 = 基础安全币（严重：50）*应用系数（核心：10）=500 安全币

贡献值对应表

应用系数/基础贡献值	严重漏洞（9~10）	高危漏洞（6~8）	中危漏洞（3~5）	低危漏洞（1~2）
核心业务（10）	90~100	60~80	30~50	10~20
重要业务（6）	54~60	36~48	18~30	6~12
一般业务（3）	27~30	18~24	9~15	3~6
边缘业务（1）	9~10	6~8	3~5	1~2

安全币对应表(安全币 ： 人民币 = 1 : 10)

应用系数/基础安全币	严重漏洞（30~60）	高危漏洞（10~28）	中危漏洞（2~8）	低危漏洞（1~2）
核心业务（10）	300~600	100~280	20~80	10~20
重要业务（6）	180~360	60~168	12~48	6~12
一般业务（3）	90~180	30~84	6~24	3~6
边缘业务（1）	30~60	10~28	2~8	1~2

三、漏洞等级说明

漏洞等级分为严重、高危、中危、低危，无影响五个级别，每个漏洞基础贡献值最高为 10，基础安全币最高为 60。 由 EMSRC 结合利用场景中漏洞的严重程度、利用难度等综合因素给予相应分值的贡献值和漏洞定级，每种等级包含的评分标准及漏洞类型如下：

严重

基础贡献值 9~10，基础安全币 30~60

额外奖励：核心业务的严重漏洞视危害程度给予额外奖励至少 10000 元人民币，且不设上限！

1) 直接获取当前业务核心服务器权限漏洞，包括但不限于内存破坏、直接上传 WEBSHELL、利用逻辑缺陷任意加载 远程代码等可利用的远程代码执行漏洞；

2) 核心敏感数据信息泄露漏洞，包括但不限于当前业务核心 DB 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；

3) 核心业务的逻辑漏洞，包括但不限于账密校验逻辑、核心接口数据验证逻辑、支付逻辑漏洞等；

4) 严重的业务逻辑缺陷，可导致：大量用户经济损失，订单及支付系统业务逻辑绕过等；

5) 严重的程序设计缺陷，可导致：大量用户敏感信息泄露，公司内部核心数据泄露等；

6) 可直接导致核心系统瘫痪的拒绝服务攻击漏洞。

高危

基础贡献值 6~8，基础安全币 10~24

1） 直接获取当前业务普通服务器或客户端权限漏洞，包括但不限于内存破坏、逻辑权限等可利用的远程代码执行漏洞；

2） 重要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；

3） 本地代码执行漏洞，包括但不限于内存破坏、类型混淆、整数问题等导致的可利 用本地代码执行漏洞；

4） 不需交互导致的重点业务漏洞，包括但不限于危害较大的存储 XSS、文件遍历、参数处理不当导致的远程拒绝服务漏洞；

5） 越权访问重要应用系统，包括但不仅限于绕过认证直接访问管理后台，后台系统密码泄露等；

6） 影响一定范围用户账号或资金安全，包括但不限于：非核心 DB SQL 入，可造成自动传播的存储型 XSS，涉及交易、资金、密码的 CSRF，可导致用户账号安全的应用系统漏洞或业务逻辑缺陷等；

7） 重要业务系统源代码、密钥或未鉴权的 API 的泄露；

8） 公司内部重要数据泄露等。

中危

基础贡献值 3~5，基础安全币 2~4

1） 需交互才能对用户产生危害的安全漏洞、包括但不限于存储型 XSS、json 劫持、CRLF、敏感操作的 CSRF 等；

2） 普通信息泄露漏洞、包括但不限于非个人登陆后泄露的手机号、姓名、交易号等个人信息；

3）远程拒绝服务漏洞，包括但不限于攻击接口、页面、组件导致的拒绝服务等；

4） 非核心业务的逻辑漏洞，包括但不限于组件导出、权限控制不当导致的 泄

露问题、重定向漏洞等。

低危

基础贡献值 1~2，基础安全币 1~2

1) 在特殊条件下才能获取用户信息的安全漏洞，包括但不限于特定浏览器下的反射 XSS、存储 XSS 等；

2) 本地拒绝服务漏洞，包括但不限于 PC 端、移动端本地组件、进程的拒绝服务；

3) 可能存在安全隐患但利用成本很高的漏洞，包括但不限于特殊情况下的中间人攻击、需要用户连续交互的敏感安全漏洞；

4) 难以利用但又可能存在安全隐患的问题。包括但不限于可能引起传播和利用的 Self-XSS 以及非重要敏感操作的 CSRF，任意 URL 重定向等；
5) 根据设备、系统、软件或框架的官方告警正在修复的漏洞。

无影响

基础贡献值 0，基础安全币 0

1) 安全无关的产品 BUG，包括但不限于产品体验或设计不好、非安全漏洞导致的服务无法访问，包括但不限于网页乱码、网页无法打开、某功能无法用等；
2) 无法利用或无危害的“漏洞”，包括但不限于恶作剧 CSRF（对用户无实际影响）、无法影响他人的本地拒绝服务 、Self-XSS、非敏感信息泄露（内网 IP、域名）等；

3) 无任何证据的猜测，非东方财富旗下产品的安全漏洞，该最终解释权归东方财富所有；

4) 基本无影响的信息泄露漏洞，包括但不限于服务器物理路径、非核心代码 SVN 文件泄漏、无危害的 phpinfo、边缘系统文件、本地日志等；

5) 公司内部普通数据泄露，如：内部　IP、系统名称等；
6) 根据设备、系统、软件或框架的官方告警正在修复的漏洞；
7) 无法利用的“漏洞”。包括但不限于没有实际意义的扫描器漏洞报告（如 Web Server 的低版本）、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF(如收藏、添加购买、非重要业务的订阅、非重要业务的普通个人资料修改等)；
8) 无任何证据的猜测；
9) 可重现且无关紧要的漏洞；
10) 根据设备、系统、软件或框架的官方告警已经修复的漏洞；
11) 已发现的漏洞，包括但不限于已知的 HTTP.sys 远程代码执行，IIS 短文件目录枚举等；
12) 关于移动安全的四大常见问题，本地拒绝服务、webview 远程命令执行、私有文件泄露、https 隐私窃取等；
13) 因业务需要，信息或数据本身是对外公开的或可查的，可忽略（比如 jsonp 劫持但无实际影响的情况等）。

四、业务系数说明

EMSRC 以业务相关性为依据，将此系数划分为四个等级：核心业务、重要业务、一般业务、边缘业务

1、“核心”业务系数为 10，参考描述：业务中涉及真实用户，资金、交易、品牌、数据等的核心业务，我司业务包括：证券、基金主站业务以及客户端，东方财富网主站以及客户端(释：业务下的核心资产，不包括资讯和模拟类页面)，涉及用户隐私数据和交易数据的管理后台；

2、“重要”业务系数为 6，我司业务包括：股吧、Choice、Level-2、期货(释：业务下的核心资产)等，以及重要的管理系统后台，邮箱系统等；

3、“一般”业务系数为 3，参考描述：业务中不涉及资金、交易、品牌、数据等的一般业务，我司业务包括：博客、东方理财师、choice 社区、财富号、东方贷、优优私募、浪客直播的主站以及客户端；三方平台的公众业务（比如旗下微信公众号、小程序）；以及非重要的证券、基金、东方财富分站，不涉及用户隐私数据和交易数据的管理后台等。

4、“边缘”业务系数为 1，一般业务中的非核心业务，包括东方财富第三方供应商提供的系统，包括：财迷、BBS 等，边缘分站、无影响的后台、非重要的测试系统等。

五、奖励方案

现金奖励处理时间：一般情况，当月申请的金币兑现，会在下月 15 日左右提现到申请时所填写的天天基金账户。

安全币：人民币=1:10

礼品商城可申请兑换人民币，以及等价值实物奖品、专属定制礼品等

为保障广大白帽子权益，兑换奖励白帽子需要告知 EMSRC 相关个人信息，如邮寄地址和联系方式；兑换现金的用户，需要提供接天天基金账户。

特别声明：安全币兑换人民币渠道，通过东方财富旗下天天基金产品活期宝形式发放给白帽子用户，由公司承担相应所得奖励的税务！最终到账金额与日期，以天天基金的账户为准，感谢理解！

5.1 奖品细则

现金：

人民币（单位:元）	对应安全币
100	10
500	50
1000	100
5000	500
20000	2000

礼品：见 EMSRC 礼品商城页面

六、评分标准通用原则

1、 奖励只针对通过 EMSRC 平台，东方财富安全应急响应微博，东方财富安全应急邮箱 security@eastmoney.com 提交漏洞的白帽子。

2、 奖励机制只支持东方财富旗下业务，合作方、供应商等第三方公司系统不在此奖励范围内。

3、 同一漏洞产生的多个漏洞，按照最高级别的漏洞奖励标准执行，漏洞数量计为一。例如：PHPwind 的安全漏洞、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、同一个 URL 多个参数的相同问题等。

4、 各等级漏洞的最终积分由漏洞利用难度及影响范围等综合因素决定，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，则可跨等级调整积分。

5、 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。

6、 漏洞挖掘过程应当以不影响东方财富旗下业务正常运作、不破坏、不传播漏洞为原则，否则东方财富有权取消漏洞奖励，并有权追究其法律责任。

7、 在漏洞未修复之前，被公开的漏洞不计分，不及安全币。

8、 网上已公开的漏洞不在奖励范围内。

9、 东方财富员工不得参与或通过朋友参与本活动。

10、以测试漏洞为借口，利用漏洞进行损 害用户利益、影响业务运作、盗取用户数据等行为的，将不计分，同时东方财富保留采取进一步法律行动的权利。

11、 漏洞奖励处理标准的解释权归东方财富所有。

12、 通用型漏洞、同一安全隐患引起的多个问题计数为一个。

13、 漏洞奖励处理标准的解释权归东方财富所有。

七、争议解决办法

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过以下三种方式联系 EMSRC 工作人员进行及时有效的沟通：

1、 邮箱 security@eastmoney.com（推荐）；

2、 微信公众号“东方财富安全应急响应中心”直接回复留言即可；

EMSRC 将按照漏洞报告者利益优先的原则处理，必要时将会引入外部安全人士共同裁定。

八、白帽子安全测试行为约束

东方财富欢迎业界安全人士在 EMSRC 平台上为我司提交安全漏洞，但反对以漏洞测试为借口，入侵业务系统、影响业务运作、窃取业务数据等有损公司利益的行为；禁止因漏洞植入后门但未上报 EMSRC 的行为，禁止测试过程中盗取大量用户敏感信息的行为，一经发现，视入侵的影响程度保留追溯其法律责任的权利。