百度安全应急响应中心漏洞奖励细节

V6.0

版本号	修订内容	发布日期
V3.0	更新评分标准；更新奖品发放流程	2015-01-23
V4.0 （试用版）	更新漏洞评分体系；新增【严重】级别漏洞评分标准；全面提升漏洞奖励力度；明确高质量漏洞奖励规则	2015-11-04
V4.0 (正式版)	优化漏洞评分体系；完善漏洞评分处理细则；取消季度奖励评选；新增月度前三现金奖励计划	2016-03-01
V4.1	提升安全币奖励系数；增加优秀团队奖励计划；优化漏洞评分通用原则	2017-04-01
V5.0	增加百度业务等级系数列表；新增威胁情报评分标准；优化优质漏洞奖励计划；优化漏洞评分通用原则；优化评分标准特殊情况声明；优化 FAQ	2018-11-01
V6.0	漏洞提交与反馈流程增加复测环节；优化无危害中漏洞评分通用原则；优化评分标准特殊情况声明；优化 FAQ	2020-11-02

目录

一、 适用范围

1. 本流程适用于百度漏洞反馈平台（sec.baidu.com 或 bsrc.baidu.com）所收到的安全漏洞报告。

2．评分标准仅适用于百度所有产品和服务，域名包括但不限于*.baidu.com、hao123.com 等。

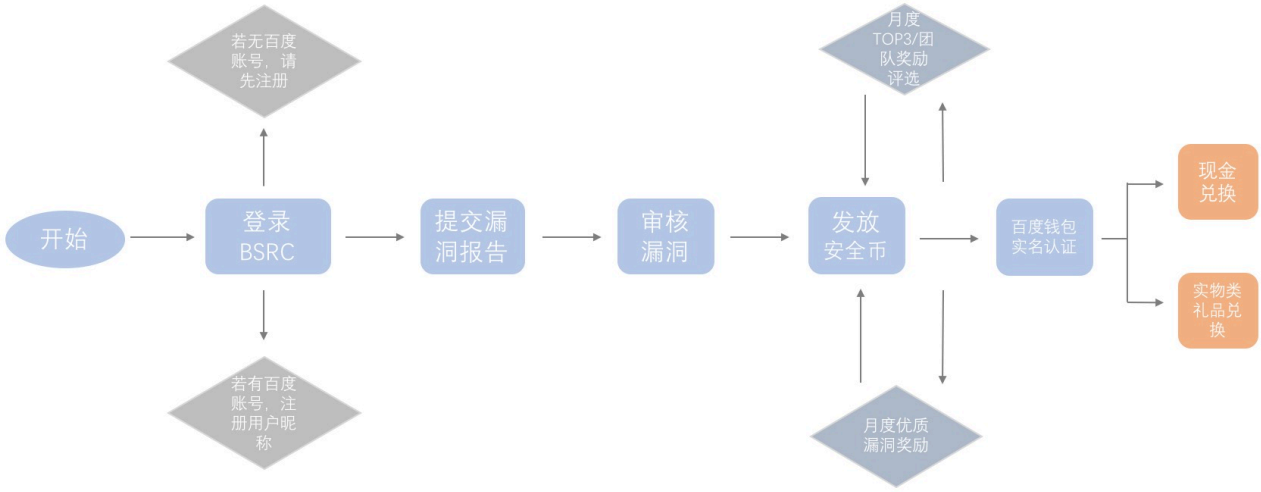
3. 同一漏洞最早提交者得分；在其它平台上提交过的不计分；与百度完全无关的漏洞不计分；提交外界已经公开的漏洞不计分。

二、 实施日期

BSRC 综合各方用户反馈及专家建议，对 V6.0 进行整理更新，包括优化漏洞评分通用原则，并于 2020 年 11 月 2 日正式执行 V6.0。

如果您对本流程有任何的建议，欢迎通过邮箱 **security@baidu.com**；微信私信@**百度安全应急响应中心（微信号 baidu_sec）**；或者通过 QQ 群 **567476227** 留言的方式向我们**反馈**。建议一经采纳，BSRC 会送出专属定制礼品。

三、 漏洞提交与反馈流程（增加复测漏洞环节）



四、 安全漏洞评分标准

根据漏洞对公司整体业务的影响程度将漏洞等级分为【严重】、【高】、【中】、【低】、【无】五个等级。每个漏洞所得**安全币数量=基础安全币*业务等级系数。**由 BSRC 结合利用场景中漏洞的严重程度、利用难度、影响范围等综合因素进行漏洞评级，并给予相应安全币，每种等级包含的评分标准及漏洞类型如下：

基础安全币 / 业务等级系数	严重（135-160）	高危（45-60）	中危（8-12）	低危（1-5）	忽略 0
高 （7-10）	945-1600	315-600	56-120	7-50	0
中 （2-6）	270-960	90-360	16-72	2-30	0
低 1	135-160	45-60	8-12	1-5	0

4.1 业务等级系数说明

业务等级系数是按照百度业务线及产品的重要性来进行划分的，分为高中低三个等级，每个等级有对应的系数范围。

注：此业务等级系数仅代表 BSRC 对具体安全问题的评分参考标准。

高等级业务产品线【本等级对应系数为 7~10】主要是包括但不限于百度战略级业务及产品线的核心域名、IP 及客户端，如：

- 百度搜索（www.baidu.com、m.baidu.com 等）
- 百度帐号系统（passport.baidu.com）
- 百度推广
- 百度无人车
- 百度 DuerOS
- 百度云
- 百度 APP

中等级业务产品线【本等级对应系数为 2~6】主要是百度重要业务产品线的域名、IP 及客户端，包括但不限于：

- 高等级业务的边缘业务线
- 百度社区服务相关产品线，如百度贴吧、百度知道、百度百科等
- 百度移动服务相关产品线，如百度输入法、百度手机卫士等
- 百度站长与开发者服务相关产品线，如百度统计、百度指数等
- 百度软件工具，如如流（原百度 hi）等

低等级业务产品线【本等级对应系数为 1】主要是除高业务等级、中业务等级以外的其他业务及产品线、百度拆分业务（子公司业务、孵化业务或已出售业务，**BSRC 只收影响百度域名的漏洞**，如**太合音乐、度小满金融等**平台的问题建议直接反馈给站点官方）

- 百度糯米
- 百度游戏
- 百度视频

备注：若目标系统是核心产品线的边缘业务（例如百度地图的某个边缘业务），并且不能获取敏感或有价值数的数据，则业务等级系数降一级（即由核心业务等级降为一般业务等级）。敏感数据包括但不仅限于大量用户数据、交易数据，或可以引起直接风险的敏感数据。且测试过程中不得获取数据，如确有必要，不得超过 10 条；严禁大规模遍历数据的行为。

4.2 【 严重 】 核心系统应用中的高危漏洞， 业务等级系数【1-10 】，基础安全币【135~160 】，本等级包括：

1. 直接获取核心系统权限的漏洞（服务器权限、PC 客户端权限）。包括但不仅限于重要业务的：远程命令执行、任意代码执行、上传获取 Webshell、SQL 注入获取系统权限，重要产品客户端缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。（注：核心系统例如 百度 passport 服务器）
2. 直接导致核心系统业务拒绝服务的漏洞。包括但不仅限于直接导致移动网关业务 API 业务拒绝服务、网站应用拒绝服务等造成严重影响的远程拒绝服务漏洞（例如可造成删除 war 包导致站点无法访问）。

3. 严重敏感信息泄漏。包括但不仅限于核心 DB（用户信息、交易信息） 的 SQL 注入，可获取大量用户的身份信息、订单信息、银行卡信息等接口问题引起的敏感信息泄露。
4. 核心系统中严重的逻辑设计缺陷和流程缺陷。包括但不仅限于通过业务接口批量发送任意伪造消息、任意账号资金消费、批量修改任意帐号密码漏洞。

【 高 】 非核心系统中的高危漏洞，或核心系统中的一般漏洞，业务等级系数【1-10】， 基本安全币【45-60】，本等级包括：

1. 属于严重级别中所描述的漏洞类型，但是产生在非核心系统中的漏洞（例如非核心系统的远程任意命令执行、可 dump 出数据的 SQL 注入），以及移动端 App 命令执行类漏洞（例如 Android WebView 远程代码执行漏洞）
2. 访问任意系统文件的漏洞，包括但不限于任意文件包含、任意文件读取。
3. 其它敏感信息泄漏。包括但不限于源代码压缩包泄漏、UC-Key 泄露、HEARTBLEED 漏洞等。同时包括通过 SVN 信息泄漏、Git 信息泄露导致的重要产品线源码泄露。
4. 包含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。
5. 包含敏感信息的越权操作及核心系统的越权操作。包括但不仅限于越权修改其他用户重要信息、进行订单操作、重要业务配置修改等较为重要的越权行为。
6. 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重要页面的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、重要操作的 CSRF，以及可获取 BDUSS 等敏感信息的各种 XSS。

【 中 】 业务等级系数【1-10】，基础安全币【8 -12 】，本等级包括：

1. 需交互方可影响用户的漏洞。包括但不仅限于一般页面的存储型 XSS。

2. 普通越权操作。包括但不仅限于越权查看非核心系统的订单信息、记录等。影响业务运行的 Broadcast 消息伪造等 Android 组件权限漏洞等。
3. 普通信息泄漏。包括但不仅限于客户端明文存储密码、客户端密码明文传输以及 web 路径遍历、系统路径遍历。
4. 普通的逻辑设计缺陷和流程缺陷。（例如绕过实名认证）
5. 其他造成中度影响的漏洞，例如：解析漏洞、目录遍历漏洞、管理后台对外

【 低 】业务等级系数【1-10 】，基础安全币【1 -5 】，本等级包括：

1. 本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等。
2. 轻微信息泄漏。包括但不仅限于路径信息泄漏、非核心系统的 SVN 信息泄漏、PHPinfo、异常信息泄露，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。
3. 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、可引起传播和利用的 Self-XSS、需构造部分参数且有一定影响的 CSRF。
4. 其他只能造成轻微影响的漏洞，反射型 XSS（包括反射型 DOM-XSS）、普通 CSRF、URL 跳转漏洞。例如：CRLF 漏洞、URL 跳转、Crossdomain.xml 配置问题。

【 无 】 基础安全币【0】，本等级包括：

1. 无法利用或利用难度较大的缺陷。包括但不仅限于 Self-XSS、无敏感操作的 CSRF、局域网中间人劫持、无意义的异常信息泄漏、内网 IP 地址/域名泄漏。

2. 任何无敏感信息的信息泄露（例如无敏感信息的 json hijacking、仅有 js、img 等的打包文件、一般信息的 logcat、包含内网 ip/域名的页面）等。
3. 无法重现的漏洞、只有“简要概述”的漏洞、不能直接体现漏洞的其他问题。包括但不限于纯属用户猜测、未经过验证的问题、无实际危害证明的扫描器结果。
4. Bos、bdysite、baidubce、aipage 等外界可以注册控制域名下的 xss 问题。

五、 威胁情报评分标准

根据情报对公司整体业务的影响程度将漏洞等级分为【严重】、【高】、【中】、【低】、【无】五个等级。每个有效情报所得**安全币数量=基础安全币*情报完整度。**由 BSRC 结合情报的危害程度、影响范围等综合因素进行评级，并给予相应安全币，每种等级包含的评分标准及类型如下：

基础安全币 / 情报完整度	严重（135-160）	高危（45-60）	中危（8-12）	低危（1-5）	忽略 0
高（7-10）	945-1600	315-600	56-120	7-50	0
中（2-6）	270-960	90-360	16-72	2-30	0
低 1	135-160	45-60	8-12	1-5	0

5.1 威胁情报等级说明

【严重】

1. 针对核心业务系统的完整入侵证据或线索，能够帮助 BSRC 对入侵事件溯源分析、定位攻击者身份。
2. 重大 0day 漏洞。如操作系统或重要组件的未公开漏洞。

3. 能对百度营收产生重大影响的相关情报。如百度搜索、商业推广等相关的大规模作弊、牟利行为。
4. 对百度产品生态有重大直接影响的黑灰产情报（如大规模盗号事件的详细情报）。

【高危】

1. 针对非核心业务系统的完整入侵证据或线索，能够帮助 BSRC 对入侵事件溯源分析、定位攻击者身份。
2. 能对百度营收产生较大直接影响的相关情报。
3. 对百度产品生态有较大直接影响的黑灰产情报。

【中危】

1. 对特定业务营收产生较大直接影响的相关情报。
2. 对百度产品生态有一定直接影响 ,或对特定业务有较大直接影响的黑灰产情报。如针对贴吧等 UGC 产品的垃圾内容作弊情报。

【低危】

1. 少量的作弊线索、黑灰产人员组织结构等相关信息。

2. 有一定影响的作弊手法。

【无】

1. 不能证实、或人为制造的等虚假或无效威胁情报。

2. BSRC 已知的威胁情报信息。

3. 不构成实际危害的情报信息。

【情报收取说明】

i. 我们鼓励提交尽量完整的情报信息，情报信息的完整度及危害程度将直接影响情报得分及漏洞评级。完整性基本信息参考 5W 1H 原则（Why What Who When Where How），即应说明何种人群在何时出于何种目的通过何种行为/业务进行谋取何种利益/危害行为。完整性低的信息泄露将可能不被视作有效的威胁情报。

ii. 同一情报最早提交者得分；无有效信息的威胁情报不计分；无法证实或伪造的威胁情报不计分；BSRC 已掌握的威胁情报不计分

iii. 我们鼓励发现如：百度 UGC 社区相关的恶意删帖、批量发黄反赌毒等恶意内容；百度账号相关的账号或个人信息泄露、恶意注册马甲号、撞库、恶意申诉等行为；百度推广广告相关账号安全、恶意推广、虚假推广等黑灰色产业链；新兴业务中的黑灰产威胁等但不限于上述业务的完整可靠有价值的安全情报。

六、 奖励发放原则

安全币用于但不仅限于礼品商城兑换礼品

漏洞报告者通过报告漏洞获得安全币，是用于 BSRC 礼品商城兑换的一种虚拟货币，**安全币数量=基础安全币*业务等级系数。**

BSRC 安全币兑换后，直接将现金发放到兑换者 BSRC 账户对应的度小满金融中，收款用户度小满金融实名认证后方可收款。

在兑换礼品前请先确认个人资料是否已完善,新版网站需要用户设置默认收件地址。如因报告者过失、快递公司问题及人力不可抗拒因素产生的奖品丢失或者损坏，后果由本人承担。

七、 现金奖励计划

1. 个人月度前三现金奖励计划

参选条件：

1） 个人月度积分达到 800 分及以上的安全专家；

2） 本月至少提交过 2 个高危或严重级别漏洞的安全专家；

获奖名单：

同时满足以上两个参选条件的安全专家有资格参与当月评选，获奖名单参照 BSRC 网站【荣誉榜】-个人排行榜。

奖励形式：

一等奖一名：5000RMB 现金奖励

二等奖一名：3000RMB 现金奖励

三等奖一名：1000RMB 现金奖励

特别说明：1) 若当月无上榜安全专家，则此奖项空缺；

2. 高质量漏洞现金奖励计划

评选条件：根据所提交高危害漏洞数量、、难易程度、影响范围、思路是否新颖等因素进行综合评选。鼓励报告者在提交漏洞报告时提供完整的漏洞发现方式，满足此条件的漏洞报告在漏洞审核中会酌情加分，并有机会参与评选高质量漏洞奖。

BSRC 将对于以下安全问题将进行**高额单独奖励**：

【重要风险情报】

1 针对百度账号的黑灰产行为 ,如盗号、恶意利用接口获取用户敏感信息(包括手机、邮箱、IP 等)等

2 针对百度核心业务如百度推广的钓鱼、作弊、欺诈等规模性的黑灰产行为

3 针对百度 UGC 社区如百度贴吧、知道、百科、百家号等的恶意刷帖、删帖等黑灰产行为

【严重类型】

1 直接远程获取核心系统权限的漏洞（服务器权限、通过百度批量获取客户端权限）

2 直接导致核心业务拒绝服务的漏洞

3 直接导致严重敏感信息泄露的漏洞

4 直接造成重大损失的严重逻辑设计或流程缺陷

5 直接造成重大损失的百度业务相关灰、黑产严重威胁情报

6 直接造成重大损失的百度技术情报及业务情报

【高危类型】

1 远程代码执行漏洞

2 高危敏感信息泄露

3 造成较大损失的百度业务相关灰、黑产严重威胁情报

4 造成较大损失的百度技术情报及业务情报

5 其他危害较大影响或范围较大的安全漏洞

【奖励规则】

i. 对于符合 BSRC 优质漏洞奖励计划的高危安全问题，将在已得评分的基础上额外给予 **1～5 万现金奖励**

ii. 对于符合 BSRC 优质漏洞奖励计划的严重安全问题，将在已得评分的基础上额外给予 **4～50 万现金奖励**

3. 优秀团队现金奖励计划

团队等级	**初识茅庐**	**掘有小成**	**移山填海**	**女娲补天**
团队人数	**>=2**	**>=5**	**>=5**	**>=5**
安全币总数	**>=1000**	**>=2000**	**>=4000**	**>=8000**
高危漏洞数	**>=3**	**>=5**	**>=10**	**>=20**
奖励	团队成员累计安全币总额 / 4	团队成员累计安全币总额 / 3	团队成员累计安全币总额/2	团队成员累计安全币总额

注：1)以上数据均为月度数据，每月度结算一次

2）对于初识茅庐队，需要两名以上队员出现在荣誉榜前 20，且总计三个以上高危漏洞，总分需大于 1000

3）对于掘有小成队，需要三名以上队员出现在荣誉榜前 15，且总计五个以上高危漏洞，总分需大于 2000

4）对于移山填海队，需要四名以上队员出现在荣誉榜前 15，且总计十个以上高危漏洞，总分需大于 4000

6)对于女娲补天队，需要三名以上队员出现在荣誉榜前 5，且总计二十个以上高危漏洞，总分需大于 8000

7）团队证书由 BSRC 统一寄给该队队长

8）对于外面已存在的团队，原则上需相关团队 leader 授权，最终解释权归 BSRC 所有

4. 增值奖励

BSRC 将加大对高质量漏洞、严重漏洞、高危漏洞的奖励力度，除上述现金奖励评选原则外，BSRC 会根据白帽子个人及团队在 BSRC 连续贡献值进行额外奖励，连续提交高危及以上漏洞的白帽子有机会获得额外惊喜。

八、 评分标准特殊情况声明

1. SSRF 漏洞不区分业务等级：完全回显计 300 分、部分回显计 40 分、无回显计 20 分。
2. 若目标系统是核心产品线的边缘业务（例如百度地图的某个边缘业务），并且不能获取敏感或有价值数的数据，则业务等级系数降一级（即由核心业务等级降为一般业务等级）。敏感数据包括但不仅限于大量用户数据、交易数据，或可以引起直接风险的敏感数据。
3. 短信轰炸的定义：单一 IP/用户半小时内定向发送超过 50 条后无任何限制。使用短信接口不受限制向不同手机发送 1 条短信的问题忽略。
4. 同一个域名的同类问题在十四个工作日内重复提交，记前三个为有效（3 个以上同类问题建议打包提交，将酌情提高评分）

5. 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。

   注：若已提交问题处于待复测状态，发现当前或其他位置仍存在该问题则重新记分

   1) 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

   2) 同一个站点多个目录存在目录浏览或 svn 信息泄露

6. 不涉及安全问题的 Bug。包括但不仅限于产品功能缺陷、网页乱码、样式混乱、静态文件目录遍历、应用兼容性等问题请提交至 help.baidu.com

7. 拒绝服务类漏洞 ,如报告中仅给出 fuzz 程序的一些调试信息、无法给出具体出现问题函数等细节，一律评 1 分

8. PC 端二进制类漏洞，需要尽可能提供 POC 和分析过程，否则将影响评分。如果该软件已经超过半年没有更新（例如百度浏览器），漏洞无危害处理

9. 通用型漏洞，如 struts 出现新漏洞，首位报告者双倍积分，报告时间一周内其他该 struts 漏洞引起的问题忽略处理，一周后如仍存在该问题则按漏洞对应级别评分

10. 在漏洞测试过程中，须遵守渗透测试原则，严格遵守《网络安全法》的规定，对于上传 webshell、反弹 shell、内网扫描探测、恶意拖取数据、下载源码等越界行为，漏洞均 0 分处理，且百度有权利报案、举报、并配合刑事侦查机关提供相应证据

11. 为了保护百度产品及业务的安全，降低用户安全风险，百度鼓励负责任地漏洞披露行为，若白帽子将未脱敏的漏洞报告向外部发布 ,或在漏洞未修复时向外界发布 ,BSRC 有权减少或取消漏洞奖励。

12. 在漏洞测试过程中，须遵守渗透测试原则，严格遵守《网络安全法》的规定，对于上传 webshell、恶意拖取数据、下载源码等越界行为，漏洞均 0 分处理，且百度有权利报案、举报、并配合刑事侦查机关提供相应证据。

13. 提交漏洞时，对提供详细漏洞触发点 url 数据包或者链接以及需要的账户权限的用户，将适当提高漏洞奖励，对报告中不贴 url 链接的，将适当扣分。

14. 对于百度不直接参与运营的业务(如百度外卖、91 助手、千千音乐、太合音乐、纵横文学、度小满金融、百度云租户等)，建议白帽子将其相关的漏洞直接反馈给该业务现在归属的公司，此类漏洞将不在 BSRC 奖励计划之内
15. 百度员工请通过内部渠道报告漏洞。一旦发现内部员工在 BSRC 提交漏洞，将把漏洞积分清零，并联系职业道德部门处理
16. 严禁社工，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，将采取进一步法律行动的权利

九、 争议解决办法（漏洞仲裁）

在用户对处理流程、漏洞评定、漏洞评分有异议的的情况下，可申请漏洞仲裁。

- 可通过邮箱： security@baidu.com 进行反馈，反馈时请附上报告者的联系方式。
- 联系 QQ 群 567476227 管理员后，会组织漏洞仲裁委员会（必要时会拉第三方介入）一起重新复审漏洞，百度安全应急响应中心将根据漏洞报告者利益优先的原则进行处理。

十、 FAQ

1. BSRC 一积分相当于多少安全币？

   安全币是 BSRC 采用的积分计量单位，可用于礼品商城的消费。按照最新调整，自 2017 年 3 月 1 日起，百度安全应急响应中心 **1 安全币=5RMB**，安全币系数由之前的 1：4 提升到 1：5。

2. BSRC 的现金兑换是怎么发放的？

BSRC 现金兑换均发放至您的 BSRC 账号对应的度小满金融里，一般兑换后 3 天内到账。

3. 我兑换了现金，可是度小满钱包里没有钱怎么办？

   若您出现这种情况，请先确认您的度小满金融已实名认证，然后联系 BSRC 工作人员。

4. 说好众测漏洞翻倍，为什么我看给分没有翻倍呢？

   为不影响月度/年度排行榜，BSRC 众测等活动的翻倍奖励将从后台为您添加。

5. BSRC 会把我交的漏洞先修复了，然后忽略我的漏洞吗？

   BSRC 承诺，所有漏洞都会得到公平、公正的处理，绝不会出现修复漏洞后不给分的情况。

6. BSRC 采用新版漏洞评分标准，会不会影响到白帽子之前的积分？

   BSRC 老用户原有积分不受任何不影响。只是以安全币代替积分作为虚拟货币单位。

7. 为什么 SQL 注入这样的高危漏洞评级会出现低危？

   评级依据该漏洞在实际场景中对业务的影响程度给出，对于同样的漏洞在不同的业务场景中会有不同的影响，其评级亦不同。（如可能出现低危的情况：只能获得有限的不敏感数据、数据库中均为公开数据）

8. 我因为工作原因向对外披露部分已修复漏洞的细节，应该怎么做、联系谁？

   若有披露已修复漏洞的需求（如有参会议题等），请至少提前一周发邮件至 security@baidu.com 说明情况，我们将评估该需求并且第一时间与你取得联系。其他情况的漏洞披露，百度将保留追究法律责任的权利。