易极付安全应急响应中心漏洞评定标准规则 V1.0

发布日期	2016-06-01
适用范围	本规则适用易极付安全应急响应中心提报的所有漏洞
有效日期	本文档发布日期至下一正式版本发布日期之前
修订记录	V1.0 首发《易极付安全应急响应中心漏洞评定标准规则》； 2016-06-01

一、基本原则

1. 我们承诺，对每一位漏洞报告者反馈的问题都有专人进行跟进、分析和处理，并给予及时答复或公告。
2. 易极付支持合作式的漏洞披露和处理，对于每位恪守白帽子精神，保护用户利益，帮助易极付提升安全质量的用户，我们将给予感谢和回馈。
3. 易极付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。
4. 易极付认为每个安全漏洞的处理与整个安全行业的进步，都离不开各方的共同合作。希望企业、安全公司、安全研究者一起加入到“合作式的漏洞披露与处理”过程中来，一起为建设安全健康的互联网而努力。

二、漏洞反馈与处理流程

【报告阶段】

白帽子通过邮件将易极付安全问题发送至漏洞接收专用邮箱：ysrc@yiji.com

【处理阶段】

1. 易极付安全应急响应中心（以下简称 YSRC）工作人员会确认收到漏洞报告并跟进开始评估问题
2. YSRC 工作人员第一时间会反馈给白帽子漏洞处理结论，必要时会与报告者沟通确认，请白帽子予以协助

【修复阶段】

业务部门修复漏洞并安排更新上线。修复时间根据问题的严重程度及修复难度而定，严重和高风险漏洞 24 小时内，中风险三个工作日内，低风险七个工作日内。

【完成阶段】

YSRC 工作人员每月定期根据白帽子所提交漏洞的实际价值，发放相应的奖品予以感谢。

三、安全漏洞评定标准

【评定标准】

根据漏洞危害程度分为严重、高危、中危、低危、忽略五个等级，每个等级涵盖的漏洞以及具体标准如下：

严重：

1. 直接获取系统权限（服务器端权限、客户端权限）的漏洞。包括但不仅限于：命令注入、远程命令执行、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. 直接导致拒绝服务的漏洞。包括通过该远程拒绝服务漏洞直接导致线上应用系统、网络设备、服务器无法继续提供服务的漏洞。

3. 严重的逻辑设计缺陷。包括但不仅限于任意账号登录、任意账号密码修改、任意账号资金消费、订单遍历、交易支付方面的严重问题。
4. 严重级别的信息泄漏。包括但不限于重要 DB 的 SQL 注入漏洞、包含配置信息等敏感信息的源代码压缩包泄漏、包含订单、用户信息的日志文件。

高危：

1. 越权访问。包括但不仅限于绕过认证直接访问管理后台可操作、核心业务非授权访问、核心业务后台弱密码等。
2. 能直接盗取关键业务的用户身份信息的漏洞。包括：重点页面的存储型 XSS 漏洞、普通站点的 SQL 注入漏洞。
3. 高风险的信息泄漏漏洞。包括但不限于普通源代码压缩包泄漏。
4. 可获取客户端权限的漏洞。包括但不限于远程任意命令执行、远程缓冲区溢出及其它逻辑问题导致的客户端漏洞。

中危：

1. 普通信息泄露。包括但不仅限于客户端明文密码存储。
2. 需交互才能获取用户身份信息的漏洞。包括但不限于反射型 XSS、JSON Hijacking、重要操作的 CSRF、普通业务的存储型 XSS。

低危：

1. 轻微信息泄露。包括但不仅限于路径信息泄露、svn 信息泄露、phpinfo、异常信息泄露。
2. URL 跳转。

无危害：

1. 不涉及安全问题的 bug。包括但不仅限于产品功能缺陷、页面乱码、样式混乱。
2. 无法利用的漏洞。包括但不仅限于 Self-XSS。
3. 不能重现的漏洞。包括但不仅限于经易极付安全应急响应中心专员确认无法重现的漏洞。
4. 纯属用户猜测的问题。
5. 非易极付集团业务漏洞。

【评定标准补充说明】

1. 评定标准仅针对易极付相关业务。目前易极付的域名包括但不限于（*.yiji.com），易极付客户端包括所有通过官方途径发布的客户端程序。
2. 提交在其他漏洞披露平台已提交的漏洞不生效。
3. 开放平台的第三方应用漏洞不生效。
4. 同一漏洞最早提交者有效。
5. 同一漏洞导致的多个利用点按照级别最高的奖励执行如：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 漏洞等等。

6. 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的,将不会生效,同时易极付保留采取进一步法律行动的权利。

【争议解决办法】

在漏洞处理过程中,如果报告者对处理流程、漏洞评定、漏洞评定标准等具有异议的 ，请通过邮件：ysrc@yiji.com 并以邮件标题【易极付漏洞处理异议】进行反馈，我们会有专门工作人员负责优先处理此类反馈。

【奖励发放原则】

我们将根据漏洞实际价值发放相应奖品予以感谢。