联想安全响应中心漏洞处理流程 V3.0

版本	内容	日期
V 3.0	更新漏洞提交入口；更新奖励评分标准；更新 FAQ	2017-4-1
V 2.0	更新奖励评分标准；更新 FAQ	2016-4-1
V 1.0	发布第一版	2015-4-1

目　　录

一. 基本原则

1. 联想对自身产品和业务的安全问题非常重视，也一直致力于保障用户安全，我们希望通过联想公司安全响应中心加强与业界个人.组织及公司密切合作，来提升联想的整体安全水平。

2. 联想对于保护用户利益，帮助联想安全提升的白帽子黑客，我们给予感谢和回馈，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。

3. 联想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资料.入侵业务系统.修改.窃取相关系统资料.恶意传播漏洞或数据。

4. 联想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.安全组织.安全研究者一起加入到"合作式的漏洞披露和处理"过程中来，一起为建设安全健康的互联网而努力。

二. 漏洞反馈和处理流程

【预报告阶段】

漏洞报告者登陆联想安全中心漏洞反馈平台 http://lsrc.vulbox.com 注册帐号。

【报告阶段】

漏洞报告者登陆联想 SRC 反馈平台，提单反馈漏洞（状态：待审阅）。

【处理阶段】

一个工作日内，联想安全响应中心（以下简称 LSRC）工作人员会确认收到的漏洞报告并跟进开始评估问题（状态：待确认）

三个工作日内，LSRC 工作人员处理问题、给出结论并计分（状态：待修复/已关闭）。必要时会与报告者沟通确认，请报告者予以协助。

【修复阶段】

业务部门修复安全漏洞并安排更新上线。

【完成阶段】

LSRC 每月第一周内，发布上月漏洞处理公告，公布月度排行榜。

三. 安全漏洞评分标准

根据漏洞危害程度分为严重、高危、中危、低危、忽略五个等级，每个漏洞所得奖励由漏洞对应用的危害程度以及应用的重要程度.利用难度.影响范围等综合因素决定：漏洞奖金=基础奖金*业务等级系数。每个等级涵盖的漏洞以及评分标准如下：

奖金（元） 业务等级系数	严重漏洞 （225~250）	高危漏洞 （150~200）	中危漏洞 （75~125）	低危漏洞 （25~50）
已声明域名 （3）	675~750	450~600	225~375	75~150
其余域名及IP （1）	225~250	150~200	75~125	25~50

声明：业务等级系数为 3 的域名包括

*.lenovo.com	*.lenovomobile.cn
*.lenovo.com.cn	*.lenovocloud.com
*.lenovomm.com	*.ecare365.com
*.lenovo.cn	*.newbd.com
*.lenovo.net	*.motorola.com
*.lenovomobile.com	*.motorola.com.cn
motorola-global-portal.custhelp.com	

【严重】

本等级包括：

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。

2. 直接导致拒绝服务的漏洞。包括但不仅限于远程拒绝服务漏洞。

3. 严重的逻辑设计缺陷。包括但不仅限于任意账号登陆.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。包括泄漏大量用户信息泄露或联想机密信息。

【高危】

本等级包括：

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用户身份信息的漏洞。重点页面的存储型 XSS 漏洞.普通站点的 SQL 注入漏洞等。

3. 高风险的信息泄漏漏洞。包括但不限于源代码压缩包泄漏。

4. 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。

【中危】

本等级包括：

1. 普通信息泄露。包括但不仅限于普调用户信息泄露。

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。

3. 需交互才能获取用户身份信息的漏洞。包括但不限于普通业务的存储型 XSS。

【低危】

本等级包括：

1. 轻微信息泄露。包括但不仅限于反射型 XSS(包括反射型 DOM-XSS)、JSONHijacking、CSRF（修改其他用户的敏感信息）、路径信息泄露、svn 信息泄露、

phpinfo、目录遍历。

2. 难以利用但存在安全隐患的漏洞。包括但不仅限于 IIS 短文件名/目录枚举。

3. 普通的逻辑设计缺陷和流程缺陷。包括但不仅限于无验证码或验证码无效。

4. URL 重定向。包括但不仅限于诱导性的 URL 跳转。

【忽略】

本等级包括：

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。包括但不仅限于经联想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。

四. 评分标准通用原则

【适用范围】

评分标准仅适用于联想产品和服务，域名包括但不限于

*.lenovo.com	*.lenovomobile.cn
*.lenovo.com.cn	*.lenovocloud.com
*.lenovomm.com	*.ecare365.com
*.lenovo.cn	*.newbd.com
*.lenovo.net	*.motorola.com
*.lenovomobile.com	*.motorola.com.cn
motorola-global-portal.custhelp.com	

服务器包括联想运营的服务器，产品包括：联想笔记本、手机、联想路由器、联想电视、联想平板、摩托罗拉手机业务。

联想全资子公司、联想投资、联想控股的公司的漏洞，以及与联想完全无关

的漏洞，不予审核通过。

【通用型漏洞】

1. 服务端：包括但不限于联想公司正在使用的 WordPress.phpcms.discuz.Flash 插件产生的漏洞，Apache 等服务端相关组件.OpenSSL.第三方 SDK 等产生的漏洞等。提交的漏洞公开时间在一个月内，联想如已从其他渠道获知，则不与审核通过；如漏洞公开时间超过一个月且存在仍未发现的漏洞，则给第一个提交者奖励，等级一般不高于中危。

2. 客户端：包括但不限于 android 原生漏洞，app 通用漏洞等。提交的漏洞公开时间在三个月内，联想如已从其他渠道获知，则不与审核通过；如联想公司仍不知情，或者漏洞公开时间超过三个月，联想仍存在未修复的漏洞，则给第一个提交者奖励，等级一般不高于中危。

【其它细则】

1. 漏洞奖励仅限于首次在联想安全响应中心反馈平台上提交的漏洞，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。

2. 同一个漏洞源产生的多个漏洞一般只给第一个提交者奖励，且漏洞数量记为一个。

3. 对于同一个链接 url，如果多个参数存在多个类似的漏洞，视情况进行合并，同一链接不同类型漏洞，按危害程度最大的给出奖励。

4. 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；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. 各漏洞的最终审核情况由漏洞利用难易程度.危害大小及影响范围综合考虑决定。

6. 拒绝无实际危害证明的扫描器结果。

【禁止以下行为】

1. 禁止以暴力枚举的方式重复对同一站点进行账号密码的猜解。如发现有未添加有效验证码可被暴力破解的站点漏洞，无论是否枚举猜解出账号密码，且此类漏洞只会按照“无有效验证码”进行确认，根据域名权重，最高按中危处理。

2. 漏洞只需证明其存在并可利用即可，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安全币。

3. 禁止以测试漏洞为借口，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，将不会审核通过，同时联想保留采取进一步法律行动的权利。

五. 奖励发放原则

自《联想安全响应中心漏洞反馈处理流程说明 V3.0》上线之日起，LSRC 将采用全新奖励体系。漏洞报告者通过报告漏洞获得奖金奖励，漏洞奖金=基础奖金*业务等级系数。

六. 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.漏洞评分等具有异议的,请通过邮件：lsrc@lenovo.com 并以邮件标题【联想漏洞处理异议】进行反馈，我们会有专门工作人员负责优先处理此类反馈。LSRC 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。

目前，联想安全漏洞反馈平台不断发展之中，可能还存在着很多需要改进和完善的地方，敬请谅解。如果您有更好的意见和想法，可以通过邮件(lsrc@lenovo.com)与我们沟通.交流。

FAQ

Q1：采用新漏洞提交系统后，白帽子在原 LSRC 平台的积分怎么办？

A：白帽子在原系统的原有积分需在 5 月 1 日前全部兑换完成，截止至 5 月 1 日，原 LSRC 平台未兑换积分将被清空。为帮助各白帽子“一分不留”，尽快兑换所有积分，原 LSRC 平台已上线 100 元京东卡兑换、10 元话费兑换等小额积分兑换商品。

Q2：在新漏洞提交系统所获得的奖金如何提现？

A：LSRC 奖金已授权漏洞盒子发放，遵循漏洞盒子奖金提现规则：提现没有时间限制，但是每次提现最低金额是 500 人民币，提现申请发出后，漏洞盒子会固顶在申请下月的 10 日打款。白帽子在提现过程中如遇奖金少发、漏发等情况，请及时联系 LSRC，联系邮箱：lsrc@lenovo.com。