金山办公安全应急响应中心

安全漏洞处理和评分标准

文件编号： KSO/P-LDPDBZ-0102-2022

编制部门： 安全中心

审批部门： 安全中心

生效日期： 2022 年 4 月 20 日

目录

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，并及时给予答复。

2．金山办公安全应急响应中心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，帮助金山办公提升安全质量的用户，我们将给予感谢和回馈。

3．金山办公安全应急响应中心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．金山办公安全应急响应中心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，共建安全健康的互联网环境，共同保护广大互联网用户。

二、漏洞流程

2.1 预报告阶段

漏洞报告者访问金山办公安全应急响应中心 https://security.wps.cn/。

如果您还没有注册金山办公在线服务账号，则需要先注册金山办公在线服务账号。

2.2 报告阶段

漏洞报告者访问金山办公安全应急响应中心，在 https://security.wps.cn/vulnerability/提交漏洞信息，提交后进入审核状态。

2.3 处理阶段

金山办公安全应急响应中心会在报告提交后的五个工作日内安全相关工作人员会处理您提交的漏洞报告。

必要时相关工作人员会与漏洞报告者沟通确认，请漏洞报告者予以协助。

2.4 完成阶段

金山办公安全应急响应中心在每季度第一周，发布上季度的漏洞处理公告，并向上季度的漏洞报告者致谢并发放礼品。

三、漏洞评定

金山办公安全应急响应中心结合漏洞危害程度、业务系数、利用难度等因素，根据国际标准 CVSS 3.0（https://www.first.org/cvss/v3-0/）进行漏洞定级和奖励计算。

3.1 业务系数

金山办公安全应急响应中心以业务重要程度为依据，将业务划分为三个等级，分别是**核心业务、一般业务、边缘业务**。

3.1.1 核心业务

核心业务系数为 10。

核心业务包括但不限于 WPS Office、金山文档、Docer 稻壳儿、金山办公账户、WPS 会员、金山 PDF、金山词霸。

3.1.2 一般业务

一般业务系数为 4。

一般业务包括但不限于业务系统运营平台、运维系统、业务分支系统、论坛社区等。

3.1.3 边缘业务

边缘业务系数为 1。

边缘业务包括但不限于一些对业务无实际影响的运维监控、测试页、测试环境、本身缺少访问权限的开源系统等。

3.2 漏洞等级

金山办公安全应急响应中心根据漏洞危害程度将漏洞等级分为【严重】、【高危】、【中危】、【低危】四个等级。

漏洞等级是根据国际标准 CVSS 3.0（https://www.first.org/cvss/v3-0/）进行评定。

3.2.1 严重漏洞

严重漏洞范围包括但不限于：

1. 直接获取基础架构系统权限包括但不限于核心业务操作系统、核心业务数据库、防火墙等。

2. 直接获取 Web 服务器权限，包括但不限于远程命令执行、上传并执行 Webshell、缓冲区域溢出等。

3. 严重的业务逻辑缺陷，可导致较大经济损失，包括订单及支付系统业务逻辑绕过等。

4. 严重的程序设计缺陷，可导致大量的用户敏感信息泄露、公司内部核心数据泄露等。

5. 可直接导致核心系统瘫痪的拒绝服务攻击漏洞。

3.2.2 高危漏洞

高危漏洞范围包括但不限于：

1. 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。

2. 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 注入，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。

3. 重要业务系统源代码、密钥或未鉴权的 API 的泄露。

4. 公司内部重要数据泄露。

3.2.3 中危漏洞

中危漏洞范围包括但不限于：

1．需用户交互且在主流浏览器中才能产生影响的漏洞，包括但不仅限于针对重要系统的普通存储型 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，身份数据篡改等。

3．少量的用户敏感信息泄露，包括但不限于客户端明文存储密码、个别用户订单或身份信息泄露等。

4．不涉及资金、订单和用户敏感信息的普通逻辑设计缺陷和业务流程缺陷。

5．可导致资源滥用或造成对用户骚扰的漏洞，包括但不限于短信炸弹、邮件炸弹等。

6．一定量的非重要系统的普通代码泄露。

3.2.4 低危漏洞

低危漏洞范围包括但不限于：

1．只在特定浏览器或客户端环境下才能执行，且影响较小的漏洞，包括但不限于反射型 XSS、非关键业务的存储型 XSS 等。

2．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。

3．低敏感度信息泄漏，包括但不限于路径泄漏、非核心代码 SVN 文件泄漏、phpinfo 等。

4．公司内部普通数据泄露，如：内部 IP、系统名称等。

5．根据设备、系统、软件或框架的官方告警正在修复的漏洞。

3.2.5 无影响

无影响范围包括：

1．无关安全的 Bug，包括但不限于网页乱码、网页无法打开、某功能无法用。

2. 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。

3. 无任何证据的猜测。

4. 不可重现且无关紧要的漏洞。

5. 根据设备、系统、软件或框架的官方告警已经修复的漏洞。

3.3 贡献值

贡献值由 CVSS 3.0 基础分、业务系数两个因素所决定。

贡献值的计算公式：

贡献值 = CVSS 3.0 基础分 x 业务系数。

3.4 安全币

安全币由 CVSS 3.0 奖励分、漏洞等级、业务系数三个因素所决定，安全币仅用于兑换礼品，不支持现金兑换。

安全币的计算公式：

安全币 = CVSS 3.0 奖励分 x 漏洞等级 x 业务系数。

3.4.1 案例

漏洞报告者报告了金山文档某处 SQL 注入，那 CVSS 3.0、贡献值、安全币的计算如下：

- CVSS 3.0 基础分 = 8.5 分（CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N）
- CVSS 3.0 奖励分 = 7.6 分（CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N/E:P/RL:O/RC:C）
- 贡献值 = CVSS 3.0 基础分 x 业务系数 = 8.5 x 10 = 85 贡献值
- 安全币 = CVSS 3.0 奖励分 x 漏洞等级 x 业务系数 = 7.6 x 3 x 10 = 228 安全币

3.5 漏洞自动忽略说明

若您提交漏洞审核未通过，我们会以留言的方式，告知您理由或需您提供更进一步详细说明，若您未及时更新补充漏洞说明，则该漏洞将被自动忽略。

四、礼品兑换

金山办公安全应急响应中心会在每月月底邮寄当月礼品。

如因漏洞报告者未能完善资料导致的延误，将顺延至下个月寄出；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，金山办公安全应急响应中心不承担责任。

五、通用原则

1. 奖励只针对通过金山办公安全应急响应中心提交漏洞的漏洞报告者。

2. 奖励只支持金山办公旗下产品或服务，接入金山办公发布的产品或服务中由合作方运营的产品及服务的漏洞不在此奖励范围内。

3. 在漏洞测试过程中，严格遵守《网络安全法》相关规定，对于利用漏洞进行损害用户利益、影响业务正常运作、盗取用户数据等行为，将不给予奖励且封号，同时金山办公安全应急响应中心有权举报并配合相关监管机关提供相应证据。

4. 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 1。

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。

5. 贡献值和安全币由金山办公安全应急响应中心根据漏洞危害程度、业务系数、利用难度等因素进行判定和计算。

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，则可跨等级调整奖励。

6. 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、重现此漏洞问题的报告者为唯一受奖励者。

7. 第三方产品漏洞，只奖励首位报告者，且不保证修复时长，包括但不限于金山办公正在使用的 Discuz、WordPress、Struts、WebLogic 等服务端相关组件以及 OpenSSL 第三方 SDK，不同版本的同一处漏洞视为相同漏洞。

8. 漏洞挖掘过程不得采用任何社会工程学方法来获取金山办公数据，否则因此对金山办公造成的损失，应承担相应的赔偿责任。

9. 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。

10. 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）。

11. 恶意提交者将封号、清空贡献值和安全币处理。

12. 在漏洞未修复之前，被公开的漏洞不计分。

13. 已公开的漏洞不在奖励范围内。

14. 金山办公员工不在奖励范围内。

15. 漏洞奖励处理标准的解释权归金山办公安全应急响应中心所有。

六、争议及解决方法

在漏洞报告处理过程中，如果报告者对漏洞流程、漏洞定级、漏洞奖励等有异议，可通过以下两种方式与金山办公安全应急响应中心工作人员联系。

1、 在漏洞详情的留言板留言；

2、 发邮件至 security@wps.cn。

金山办公安全应急响应中心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。