网络安全 FCIS 2023 创新大会

基于供应商安全能力考核的供应商评估体系

供应商安全评估实务

千寻位置 王忠惠

FREEBUF

安全威胁不止开源软件

金山办公 KINGSOFT OFFICE

安全通告

安全通告 - WPS Office 存在代码执行漏洞

通告编号	WPSSRC-2023-0701	初始发布时间	2023-07-28
		更新发布时间	2023-07-28

摘要

WPS Office 软件是由金山办公软件股份有限公司自主研发的一款办公软件套装，可以实现办公软件最常用的文字、表格、演示等多种功能，覆盖 Windows、macOS、Linux、Android、iOS 及鸿蒙等平台。

目前该漏洞已成功地得以修复，并已发布了相应的安全版本。

请用户尽快升级至安全版本，以完成该漏洞的修复工作。WPS Office 个人版已推出热补丁，用户可通过重启 WPS Office 以自动更新热补丁来完成修复工作。

影响范围

受影响软件名称及版本：

软件名称	平台	版本号
WPS Office 个人版	Windows	低于 12.1.0.15120（含）
WPS Office 机构版本（如专业版、专业增强版）	Windows	低于 11.8.2.12055（含）

供应链安全管理的不足

供应商审查

缺少全面的审查流程，或无深入评估安全实力和合规性

透明度管理

不了解供应链的运作，未准确识别合作伙伴导致的风险

漏洞与响应

不及时的漏洞检测、通知和修补，不健全的应急响应计划

意识与合规

安全意识不一致，未能充分掌握合规性要求，潜在监管

潜在的安全风险

技术漏洞

安全功能不足
隐私设计缺失
数据保护不到位
后门及恶意逻辑
网络防御匮乏

人员意识

社会学攻击
安全意识
竞对窃取
商业泄密

法律不合规

缺失NDA
责任条款模糊
违背法律

原型保护

无关键人员清单
无物理安全措施
无监控保护
无事件告知和恢复

业务中断

经营水平差
安全能力差
易被黑客掌握

如何理解供应链安全要求

1 《网络安全法》及相关法律

- 安全管理责任
- 开展安全评估
- 个人信息保护
- 重要数据出境
- 事件应急处置

2 ISO信息安全标准体系

- 供应商评估活动
- 供应链分析管理
- 个人信息影响评估
- 信息共享和传递
- 供应链审计

3 等保、密评、关保等测评

- 供应链安全
- 应急响应能力
- 供应商管理

供应商的选择

业务匹配	口碑声誉	透明度	技术能力	体系认证	商务条款
最低的需求点	行业影响力	关键技术	先进性	公司管理文化	SLA承诺
最严格的要求	同行评价	关键服务	可靠性	公司安全文化	责任及赔偿
避免迷魂汤	用户交流	技术来源	研发人员	安全管理体系	保密性
	公开性事件	OpenAPI	服务人员	隐私保护体系	低成本
		定制性	及时性	产品服务质量	

供应商准入管理

准入

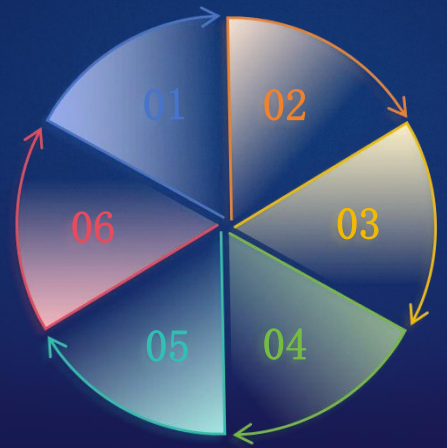
采购分析
供应商招募
供应商资质审查

退出

供应商分类
供应商替代或淘汰

改进

供应商质量提升
供应商能力赋能



寻源

招投标
竞价与选择
三方寻源

过程管控

合作执行
交付监控
风险追踪

综合评估

综合能力考核
供应商能力培训

开展评估的时机

准入
- 项目立项
- 需求评审
- 确认标准

01

过程
- 资质认证
- 测试验证
- 交付审核

02

定期
- 培训
- 评估
- 考核

03

改进
- 评级提升
- 问题追踪

04

供应商安全能力考核体系

01 **合约协议**

NDA、安全责任书、数据处理协议、隐私保护协议、落实情况

02 **体系认证**

安全体系认证、网络数据安全体系、年度安全计划、安全机构和执行记录

03 **研发安全**

产品安全基线、SDL过程、渗透测试、安全控制机制证明、数据流图、日志

04 **质量测试**

问题管理、接口和中间件清单、私有协议识别、测试覆盖与回归

05 **软件供应链**

商业软件、开源软件、组件合规清单、版本管控机制

06 **安全生产**

稳定性管理、安全管理活动、上线安全卡发

07 **交付安全**

交付物安全管控、完整性和版本管控、数据安全活动、作业记录、事件响应

08 **隐私保护**

隐私保护政策、个人信息影响性分析、隐私培训、数据出境、奖惩

09 **漏洞应急**

SRC、漏洞披露、漏洞定级处置、漏洞响应流程

10 **审计溯源**

台账

11 **人员管理**

人员招聘周期管控、关键人员岗位识别

12 **原型保护**

商业保密机制

考核与监督的挑战

培训

赋能

退出

供应链安全展望

提供数字安全透明性，
跨界协同机制

供应商能力成熟度测
评及服务

数字化转型

AIGC

专业机构

智能化有利于探索供
应链风险

网络安全 FCIS 2023创新大会

THANKS

FREEBUF