2023 年网络与信息系统安全月报
（9 月）

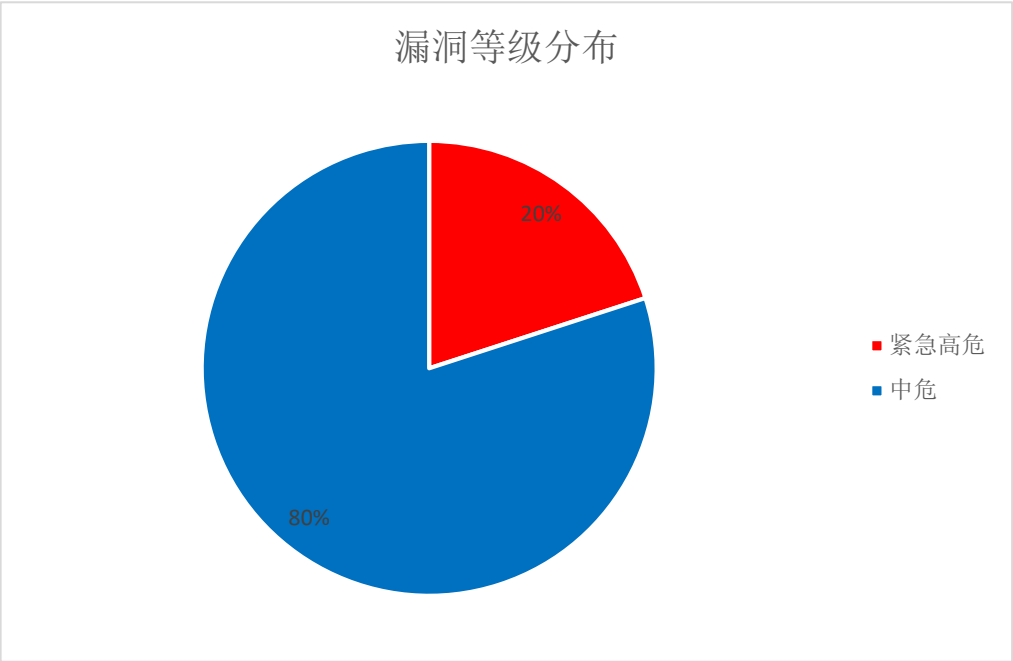
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 9 月份网络与信息系统安全情况通报如下：

一、本月整体安全情况

（一）漏洞发现情况

本月共发现漏洞 14 个。通过在校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 10 个，校外通报漏洞 1 个，外链 3 个。其中紧急高危 3 个，中危漏洞 11 个，低危漏洞 0 个，紧急高危占比：20%。紧急、高危、中危、低危漏洞统计情况见下图：



注：

紧急高危漏洞是指可远程利用并能直接获取系统权限（服务器端权限、客户端权限）或者能够导致严重级别的信息泄漏（泄漏大量用户信息或学校机密信息）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、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权访问、核心业务后台弱密码等。

中危漏洞是指能直接盗取用户身份信息或者能够导致普通级别的信息泄漏的漏洞，包括但不限于目录浏览、客户端明文密码存储等。

低危漏洞是指能够导致轻微信息泄露的安全漏洞，包括但不仅限于 web 页面错误、堆栈信息泄露、JSONHijacking、CSRF、路径信息泄露、SVN 信息泄露、phpinfo 等。

（二）第三方漏洞通报

本月第三方漏洞通报均在规定时间内完成处理，未造成网络安全事件。

通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
江苏省委网信办	218.94.19.58	弱口令	已修复	智能制造研究院

（三）非法外链情况

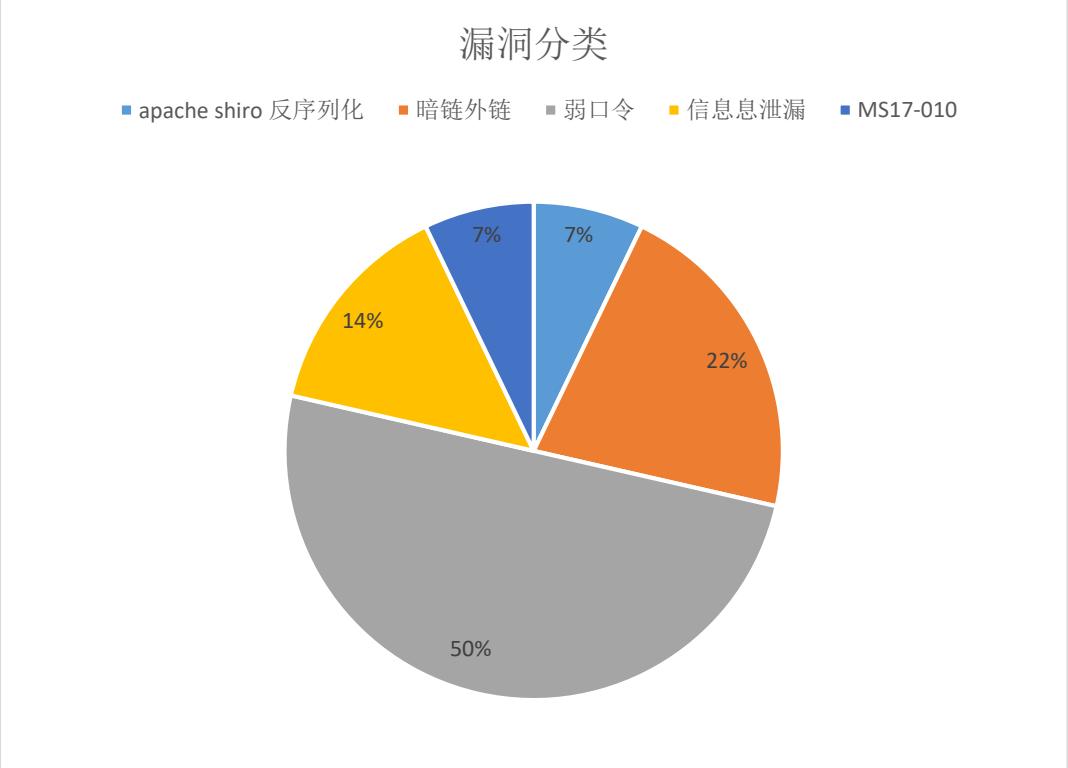
本月检查到 2 家单位所属网站共出现 3 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://zjy.njtech.edu.cn	马克思主义学院	1 次	通信管理局
https://kyy.njtech.edu.cn	科学研究院	2 次	通信管理局

二、安全情况分析

（一）漏洞类型统计

本月共发现漏洞 14 个。其中暗链外链漏洞 3 个、弱口令漏洞 7 个、信息息泄漏漏洞 2 个、MS17-010 漏洞 1 个、apache shiro 反序列化漏洞 1 个。漏洞分类占比如下图：



（二）漏洞修复统计

本月共发现漏洞 14 个，均已修复。

（三）2023 年网络安全宣传周

2023 年国家网络安全宣传周于 2023 年 9 月 11 日-17 日开展。根据《省教育厅办公室关于开展 2023 年江苏省教育系统网络安全宣传周校园日活动的通知》（苏教办信函〔2023〕10 号）要求，学校组织开展了 2023 年南京工业大学国家网络安全宣传周校园

日系列活动，包括校园日直播活动、钓鱼邮件安全演练、网络安全应急演练、新生校园网络使用专题培训、网络反诈主题活动等。

学校网络安全宣传周校园日活动连续开展，师生参与度越来越高，影响力和覆盖面越来越大，目前已成为我校网络安全宣传教育的重要平台，大力提升了师生网络安全意识和防护能力，推进了网络安全知识进校园、进课堂、进头脑。

（四）网络安全攻防演练

为提高全校师生网络安全意识和防范技能，妥善应对和处理重要信息系统突发事件，确保能在最短时间内，及时、果断处理危害网络与信息安全的突发事件，防止造成重大损失和影响，提高各部门网络与信息系统应急保障和处置能力，9 月 20 日，信息管理中心根据学校信息化年度工作安排进行了网络安全攻防演练。此次演练针对我校信息系统出现较多的弱口令、命令执行以及服务器未打补丁导致失陷等漏洞展开，演练对象为：档案馆的档案管理系统（202.119.243.253），后勤保障处的智慧后勤（http://202.119.242.100:8081）以及教务处的教务系统（202.119.248.202），在演练过程中，三个系统均被攻陷。演练过程中涉及部门均在规定时间内对相关系统进行了处理。

本次网络安全应急演练活动是 2023 年南京工业大学国家网络安全宣传周校园日系列活动的重要组成部分，此次演练聚焦学校重点网站、重要信息系统的实体安全、运行安全和数据安全，模拟在面对网络安全突发事件时，如何妥善应对处置，最大限度地减少事件产生的危害，维护学校网络安全。通过实战演练，进

一步强化了各单位网络安全防护意识，以及对网络安全隐患的发现力、研判力和应对力。

（五）网络安全邮箱钓鱼演练

本月，为提高师生对钓鱼邮件的甄别能力，切实体会钓鱼邮件的迷惑性和隐蔽性，根据工作安排，信息管理中心牵头开展了面向全校师生的钓鱼邮件演练活动。

本次活动选取了全校师生学校邮箱作为演练对象，为教师和学生精心设计了以 ChatGPT 为钓鱼邮件主题的演练内容。为确保活动的顺利进行，相关人员提前进行了充分的准备工作，确保了演练的高效进行。

本次钓鱼邮件演练共有本次邮箱钓鱼演练共发送邮件 40549 封， 打开邮件 2967 人，点击链接 993 人，提交数据 680 人。令人欣慰的是，大部分师生都看穿了钓鱼邮件的“伪装”，没有进一步填写个人信息，而是积极地向信息管理中心反馈和举报，充分体现了我校师生良好的网络安全意识。

网络安全形势严峻且极具挑战，境外不法分子常暗中窥探，因此我校师生对于邮件安全的关注度亟待提高。未来，信息管理中心将继续加大网络安全宣传力度，积极开展各类安全教育活动，提高师生的网络安全意识和自我防护能力，为构建和谐安全的网络环境贡献力量。

三、安全威胁风险与防范

（一）传统威胁防范

安全威胁风险	防范措施建议
弱口令较多	加强人员网络安全防范意识，定期修改网站登录密码。
网页存在暗链外链	定期排查网页外链，清除过期链接，避免被恶意抢注为非法网站。
网站配置文件泄露	服务器禁止备份网站文件，禁止将配置文件泄露到公网，加强网站访问目录权限限制。

（二）QQ Windows 客户端存在远程代码执行漏洞的预警

1．漏洞描述

经有关单位通报，QQ Windows 客户端 9.7.13 及之前版本存 在远程代码执行漏洞，攻击者利用漏洞可通过转发消息的形式传播恶意代码，在被攻击者点击消息内容时，恶意代码将被自动下载执行。

目前腾讯已紧急发布 QQ Windows 客户端 9.7.15 版本，修复了该漏洞。请各单位排查 QQ Windows 客户端使用情况，及时升级版本修复漏洞，并加强安全防范，不要点击聊天窗口的不明网络链接。

2．影响范围

QQ Windows 客户端 9.7.13 及之前版本

3．修复建议

修复版本链接：https://im.qq.com/pcqq。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，因各部门响应处理及时，未造成网络安全事件。各单位要种好“责任田”，强化组织领导，履行主体责任，加强宣传教育；信息系统建设者要筑好“防火墙”，全面加强网络安全保障体系和能力建设，全力保障信息系统安全和数据安全；广大师生要当好“守门员”，增强网络安全意识和能力，遵守相关法律法规，争做网络安全的参与者、守护者和贡献者。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023 年 10 月 7 日