2023 年网络与信息系统安全月报
（7-8 月）

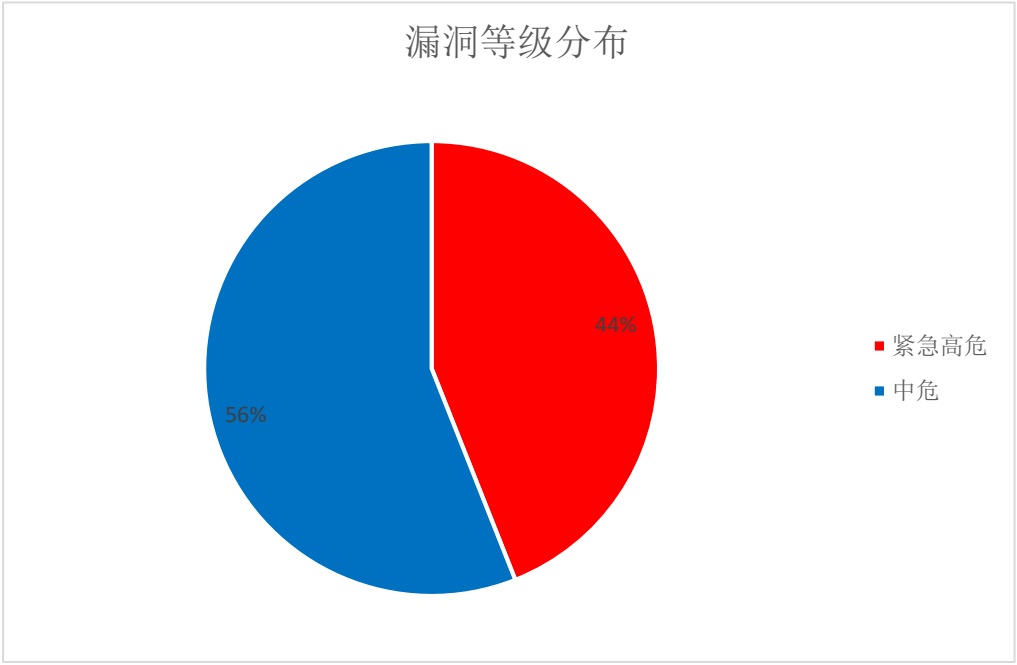
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将7-8 月份网络与信息系统安全情况通报如下：

一、本期整体安全情况

（一）漏洞发现情况

7-8 月共发现漏洞 50 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 20 个，校外通报漏洞 13 个，外链 17 个。其中紧急高危 22 个，中危漏洞 28 个，低危漏洞 0 个，紧急高危占比：44%。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

7-8 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
江苏省教育网信办	xsgl.njtech.edu.cn	弱口令	已修复	学生工作处
江苏省教育网信办	jkdk.kooci.net（双非系统）	弱口令	已关闭	人事处
江苏省教育网信办	xsgl.njtech.edu.cn	文件上传	已修复	学生工作处
江苏省教育网信办	hqjd.njtech.edu.cn	目录浏览	已修复	后勤保障处
江苏省教育网信办	alstu.njtech.edu.cn	非预期文件上传漏洞	已修复	学生工作处

江苏省教育网信办	alstu.njtech.edu.cn	未授权访问	已修复	学生工作处
江苏省教育网信办	njtech.bcplab.com（双非系统）	远程代码执行漏洞	已修复	柔性电子（未来技术）学院
江苏省教育网信办	202.119.248.18	目录浏览	已关闭	后勤保障处
江苏省教育网信办	zhgh.njtech.edu.cn	逻辑缺陷漏洞	已修复	工会
教育 SRC	zrb.njtech.edu.cn	水平越权	已修复	学术期刊编辑部
教育 SRC	rlcj.njtech.edu.cn	未授权访问	已修复	保卫处
南京市公安局	virtual-a.cge.njtech.edu.cn	未授权访问	已关闭	测绘科学与技术学院
南京市公安局	virtual-a.cge.njtech.edu.cn	多个弱口令	已关闭	测绘科学与技术学院

漏洞通报来源：江苏省教育网信办（“网安 2023”教育系统网络安全保障专项行动），教育 SRC 平台，南京市公安局。

（三）非法外链情况

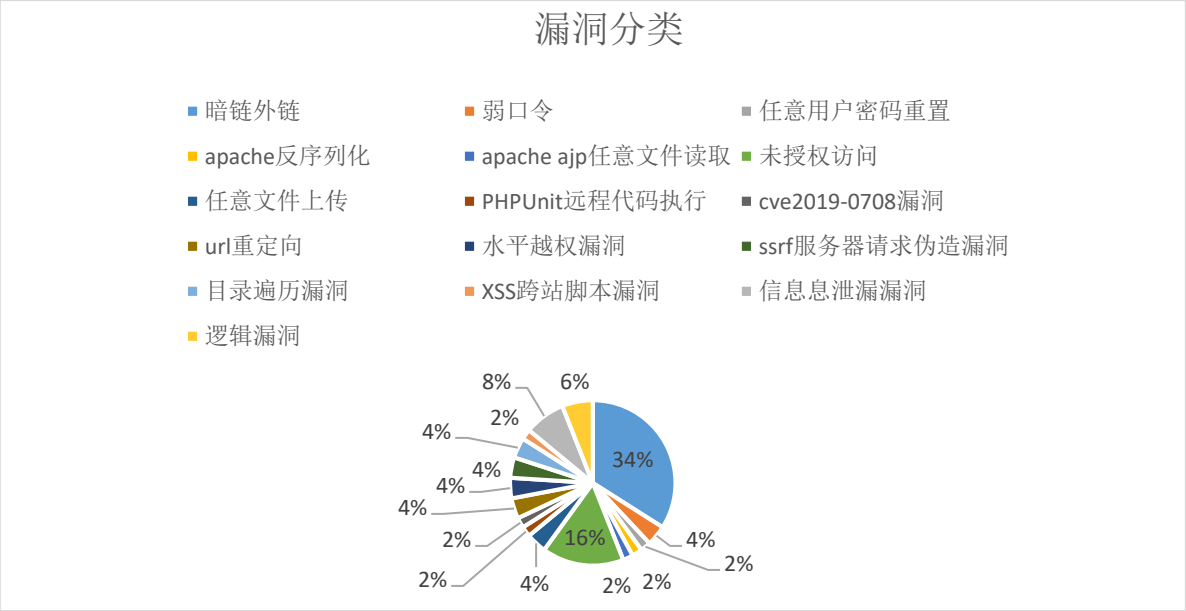
7-8 月检查到 3 家单位所属网站共出现 17 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://tyxy.njtech.edu.cn/	体育学院	3 次	校内自查
http://maker.njtech.edu.cn	教务处	1 次	通管局
https://kyy.njtech.edu.cn	科学研究院	13 次	通管局

二、安全情况分析

（一）漏洞类型统计

本期共发现漏洞 50 个。其中暗链外链 17 个，弱口令 2 个，任意用户密码重置漏洞 1 个，apache 反序列化漏洞 1 个，apache ajp 任意文件读取漏洞 1 个，未授权访问 8 个、任意文件上传 2 个、PHPUnit 远程代码执行 1 个、cve2019-0708 漏洞 1 个、url 重定向 2 个、水平越权漏洞 2 个、ssrf 服务器请求伪造漏洞 2 个、目录遍历漏洞 2 个，XSS 跨站脚本漏洞 1 个、信息息泄漏漏洞 4 个、逻辑漏洞 3 个。漏洞分类占比如下图：



（二）漏洞修复统计

7-8 月共发现漏洞 50 个，均已处理。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
逻辑漏洞和信息泄漏	系统管理员需提高对厂商的要求，提高厂商对自身系统页面逻辑性判断，增强厂商的网络安全意识，保护学校数据。
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。
未授权访问	系统管理员需提高对厂商的要求，增强厂商的网络安全意识，保护学校数据。
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。

四、网信安全每月小结

7-8 月我校信息系统漏洞总数量较多，因各部门响应处理及时，未造成网络安全事件。各单位需要进一步压实信息系统管理责任，长时间不更新维护的网站和系统须及时关停，加强对“双非”系统的管理，全面梳理本单位所属“双非”系统资产，新增“双非”系统要及时签订“双非”系统安全责任书，做好“双非”系统安全防护和应急预案，防止出现安全问题。各单位在开学期间要加强网络安全工作组织部署，积极开展网络安全隐患排查和整改，切实做好安全监测预警通报工作，建立网络安全应急响应机制，加

强值班值守和信息报送，确保全校网络与信息系统持续安全稳定，顺利完成开学期间的网络安全保障工作。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023 年 9 月 6 日