2022 年网络与信息系统安全月报

（7 月）

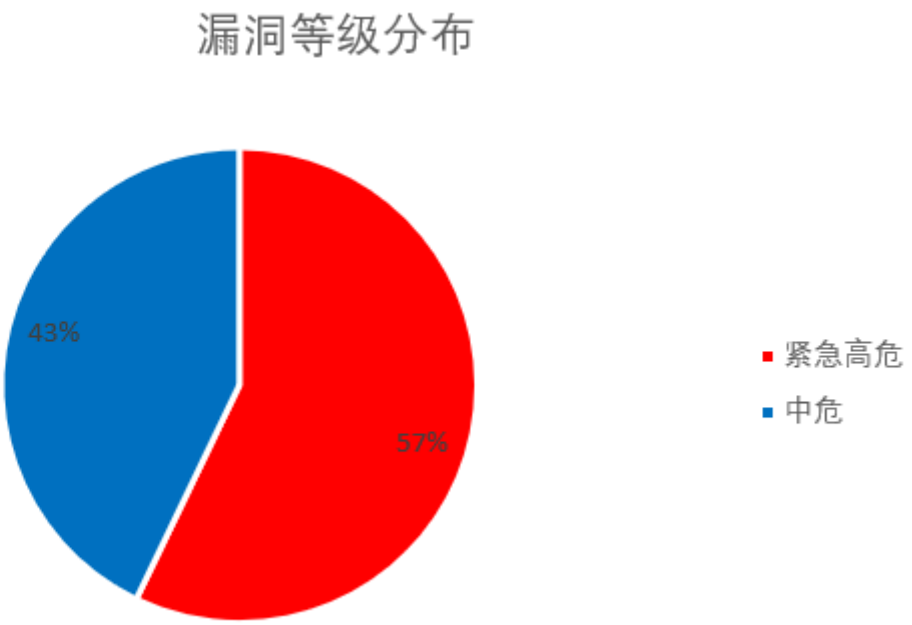
各单位、各部门：

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 月份网络与信息系统安全通报如下：

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 13 个，校外通报漏洞 1 个。其中紧急高危 8 个，中危漏洞 6 个，低危漏洞 0 个，紧急高危占比：57%。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

本月所有漏洞通报均在规定时间内完成处理，未造成网络安全事件。

漏洞通报的来源：江苏省教育网信办。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
江苏省教育网信办	jfpt.njtech.edu.cn	跨站脚本	已修复	计划财务处

(三)非法外链情况

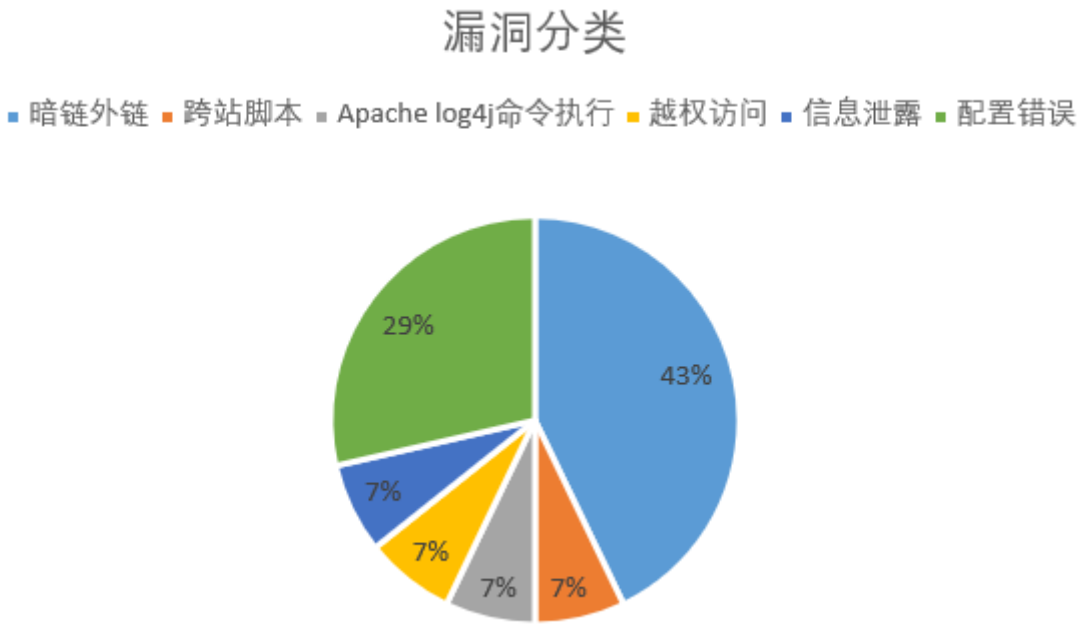
本月检查到 5 家单位所属网站共出现 6 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://cqt.njtech.edu.cn/	党委宣传部	1 次
http://jwc.njtech.edu.cn/	教务处	1 次
http://cly.njtech.edu.cn/	材料科学与工程学院	2 次
http://jszy.njtech.edu.cn/	大学科技园管理办公室	1 次
http://life-phar.njtech.edu.cn/	生物与制药工程学院	1 次

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 14 个。其中暗链外链 6 个，跨站脚本 1 个，Apache log4j 命令执行 1 个，信息泄露 1 个，越权访问 1 个，配置错误 4 个。漏洞分类占比如下图：



(二)漏洞修复情况

本月发现的漏洞均已修复。

三、安全威胁风险与防范

(一) 传统安全威胁风险与防范

安全威胁风险	防范措施建议
网站暗链外链较多	定期清理过期新闻公告，定期进行暗链外链扫描。
系统对外不必要开放注册接口	梳理自身网站注册接口，非必要对外业务尽量关闭注册功能。

（二）挖矿病毒防范

为加强对挖矿病毒的防范，信息管理中心本月在防火墙上对6个境内外矿池地址进行了封禁，有效地避免了挖矿病毒对我校正常网络服务造成影响。今后学校将继续加强对挖矿病毒的技术检测和防范，持续对挖矿行为保持高压打击态势，保护师生网络安全。

（三）个人数据安全保护

为做好校内师生个人数据保护，根据《数据安全法》和《个人信息保护法》，信息管理中心组织开展了个人信息数据安全保护专项行动，全面摸排各单位自建的涉及使用大量个人信息的信息系统，要求各单位对信息系统安全风险进行评估，完善存储大量个人信息的信息系统清单，明确服务外包的网络和信息安全管理责任，落实签订保密责任协议，全面降低信息系统的数据泄露风险。

四、网信安全每月小结

本月我校信息系统漏洞总量较少，因响应处理及时，未造成网络安全事件。但网页暗链外链情况比较严重，请各单位、各部门加强网页安全管理，及时删除过期通知公告。要严格落实安全管理职责，做好风险防控，确保全校网络与信息系统持续安全稳定。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022年8月10日