2021 年网络与信息系统安全月报

（12 月）

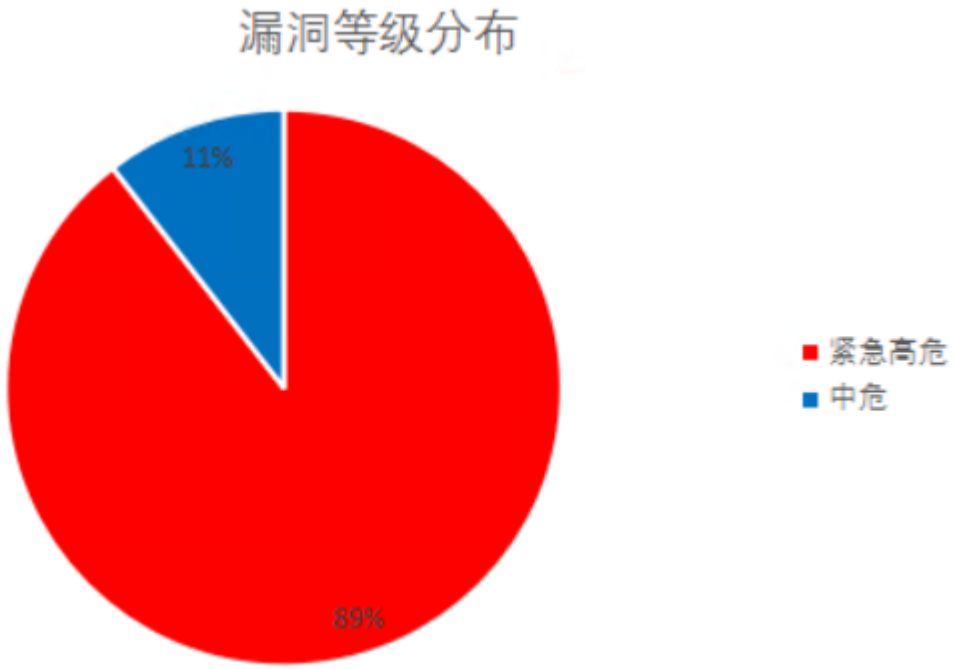
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 12 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 19 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 17 个，校外通报漏洞 2 个。其中紧急高危 17 个，中危漏洞 2 个，低危漏洞 0 个，紧急高危占比：89.5%。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。

漏洞通报的来源包括：教育 SRC、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
教育 SRC	https://jwgl.njtech.edu.cn/xtgl/	Apache log4j 远程命令执行	已修复	教务处
江苏省教育网信办	http://gra.njtech.edu.cn	信息泄露	已修复	研究生院

(三)非法外链情况

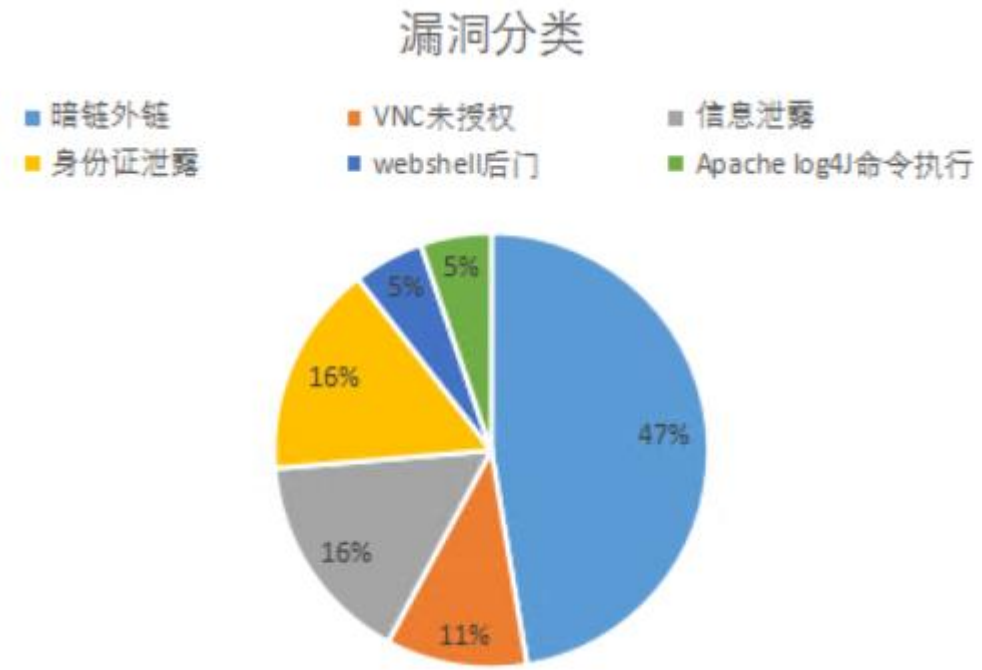
本月检查到 6 家单位所属网站共出现 9 次非法外链，具体情况如下：

网站（系统）	部门
http://green.njtech.edu.cn/	计算机科学与技术学院
http://pharm.njtech.edu.cn/	药学院
http://tyxy.njtech.edu.cn/	体育学院
http://life-phar.njtech.edu.cn/	生物与制药工程学院
http://dgy.njtech.edu.cn/	电光源材料研究所
http://cces.njtech.edu.cn/	安全科学与工程学院

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 19 个。其中暗链外链 9 个，VNC 未授权 2 个，信息泄露 3 个，身份证泄露 3 个，webshell 后门 1 个，Apache log4j 命令执行 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 12 月共发现漏洞 19 个，本月漏洞均已修复。

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
身份证泄露	发布新闻附件中禁止填写身份证信息，如必须填写，必须将出身日期和最后两位模糊化。
暗链外链	加强扫描力度，定期清除过期的新闻公告。
托管服务器缺少防护	托管服务器迁移到校内统一防护
敏感端口存在紧急漏洞	不必要对外端口只限制本地访问，不对外访问

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。本月我校受挖矿病毒威胁状况明显改善，但暴露的传统网络安全问题仍需要高度重视，网站暗链外链数量较多，重要系统存在敏感信息泄露问题，特别是敏感端口对外开放，对网站（系统）正常运行造成很大安全隐患，需要各单位重点关注。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 1 月 4 日