2022 年网络与信息系统安全月报

（5 月）

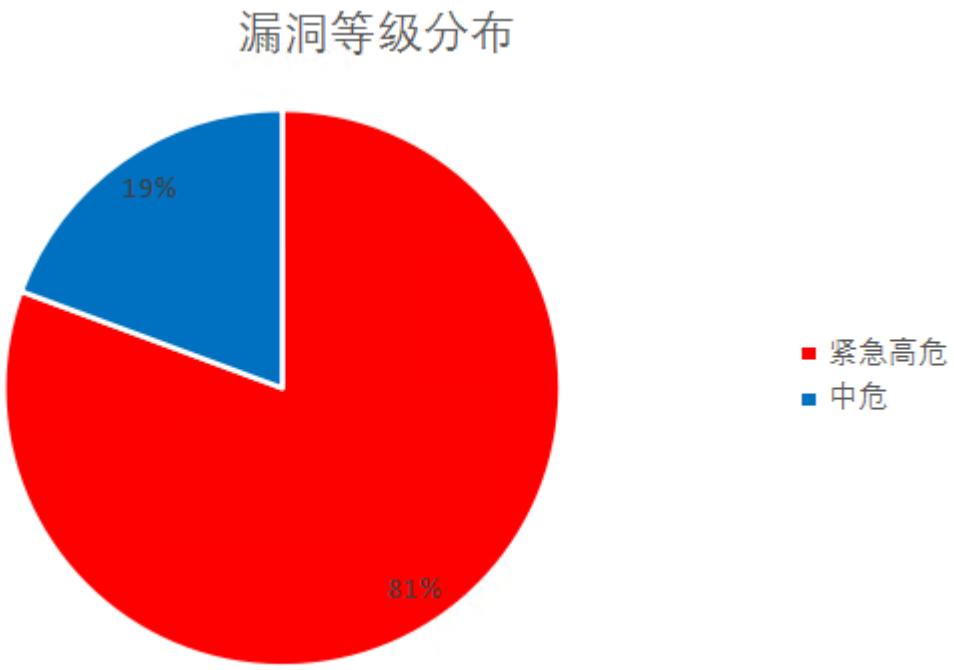
各单位、各部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 5 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 31 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 30 个，校外通报漏洞 1 个。其中紧急高危 25 个，中危漏洞 6 个，低危漏洞 0 个，紧急高危占比：80.6%。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。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 SRC	http://virtual-a.mech.njtech.edu.cn	弱口令	已修复	机械与动力工程学院

(三)非法外链情况

本月检查到 11 家单位所属网站共出现 16 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://art.njtech.edu.cn	艺术设计学院	1 次
http://trans.njtech.edu.cn	交通运输工程学院	1 次
http://2011college.njtech.edu.cn	2011 学院	2 次
http://spy.njtech.edu.cn	食品与轻工学院	1 次
http://tyxy.njtech.edu.cn	体育学院	1 次
https://alumni.njtech.edu.cn	对外合作与发展处	1 次

http://lib.njtech.edu.cn	图书馆	1 次
http://pharm.njtech.edu.cn	药学院	1 次
http://hgy.njtech.edu.cn	化工学院	5 次
http://mce.njtech.edu.cn	材料化学工程国家重点实验室	1 次
http://dgy.njtech.edu.cn	电光源材料研究所	1 次

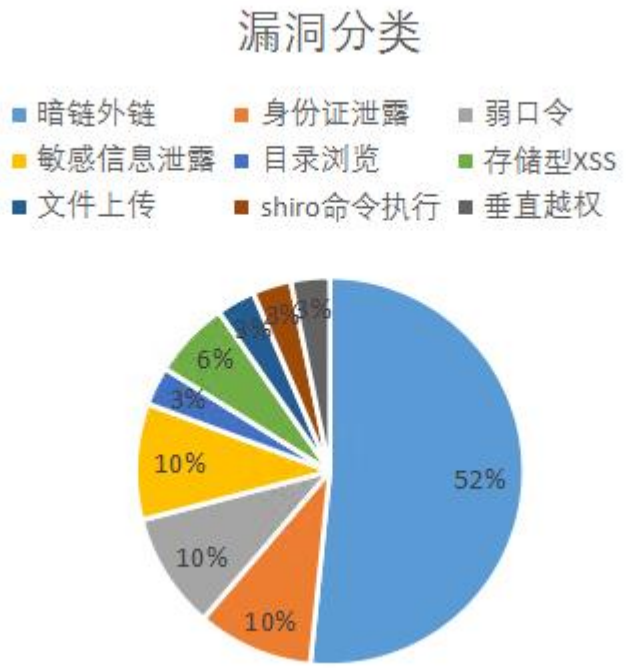
（四）排查非法外链

针对本月非法外链漏洞数量增加的情况，信息管理中心立即开展了安全防护工作，利用技术手段对各二级单位、部门网站的高频非法外链地址进行专项排查整治，共发现 63 条非法外链记录，并立刻进行了批量删除。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 31 个。其中暗链外链 16 个，身份证泄露 3 个，弱口令 3 个，敏感信息泄露 3 个，目录浏览 1 个，存储型 XSS 2 个，文件上传 1 个，shiro 命令执行 1 个，垂直越权 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

本月漏洞均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
网页存在身份证泄露	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。
学校系统弱口令较多	加强系统负责人安全管理意识，普及弱密码危害，定期修改管理员密码。
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。
系统存在可执行命令漏洞	加强漏洞扫描力度，出现紧急漏洞及时修复，避免漏洞被恶意利用。

四、网信安全每月小结

本月我校信息系统漏洞总量较多，各部门响应处理及时，未造成网络安全事件。本月我校暗外链、弱口令和信息泄露

等传统网络安全漏洞数量明显增加。各单位要建立常态化的网络与信息系统安全检查机制，定期对本单位负责的网站和信息系统进行检查，加强附件内容审核，发现问题及时上报，及时整改，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 6 月 9 日