2021 年网络与信息系统安全月报
（10 月）

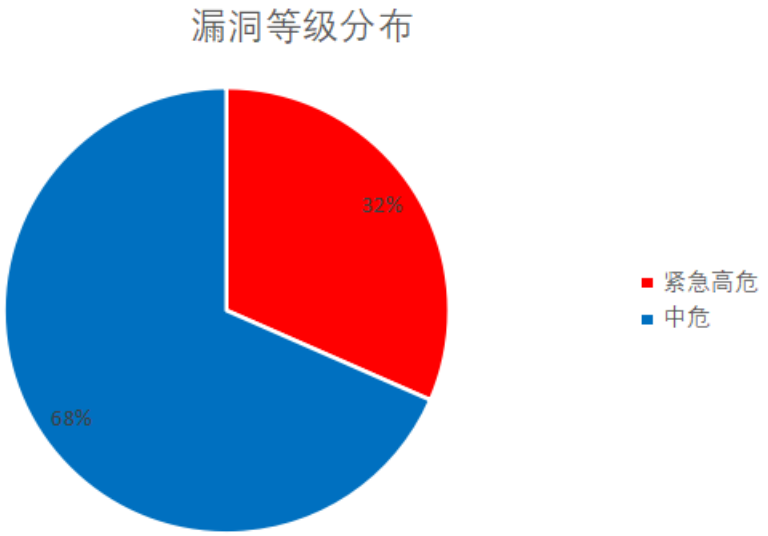
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 10 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 20 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 18 个，校外通报漏洞 2 个。其中紧急高危 6 个，中危漏洞 14 个，低危漏洞 0 个，紧急高危占比：33%。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。漏洞通报的来源为：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	libwx.njtech.edu.cn	HTTP Slow 漏洞	已修复	图书馆
江苏省教育网信办	58.213.118.183	挖矿病毒	已修复	个人

(三)非法外链情况

本月检查到 3 家单位所属网站共出现 4 次非法外链，具体情况如下：

网站（系统）	部门
http://nthy.njtech.edu.cn/	化工学院
http://green.njtech.edu.cn/	计算机科学与技术学院
http://maker.njtech.edu.cn/	教务处

(四)挖矿病毒专项检查

本月，江苏省发改委组织力量对江苏省高校感染挖矿病毒情况进行了专项检查及处理。本次检查共发现了我校受感

染的个人电脑 IP 共 9 个。具体情况如下：

姓名	身份	中毒电脑 IP	所属部门
赵**	学生	10.26.16.95	化工学院
付**	学生	10.26.16.13,10.26.16.38	化工学院
张**	学生	10.22.245.112,10.26.16.76	化工学院
陶**	学生	10.7.26.74	化学与分子工程学院
朱**	教师	10.10.136.19	先进材料研究院
胡**	教师	10.13.46.141	生物与制药工程学院
谢**	学生	10.13.116.92	机械与动力工程学院

信息管理中心对这些受感染设备立即进行了紧急网络隔离，并通知设备所属人员和部门，对设备进行全面病毒查杀和修复，避免了校内大规模挖矿病毒感染情况的发生，确保校内电脑终端正常运行。下一步,信息管理中心将持续开展虚拟货币“挖矿”态势分析，并进一步联合各相关部门，形成“多维度、多层次”的处置体系，配合做好违法虚拟货币交易的溯源与打击。

（五）图书馆网络安全事件复现

网络安全事件复现：某系统（网站）存在的安全事件，在得到有效处理后，再次被主管部门监测或检查发现。

2021 年 10 月 14 日，我校接江苏省教育网信办通报，我校图书馆所属系统 libwx.njtech.edu.cn 存在 HTTP Slow 漏洞，该漏洞为 2021 年 6 月 9 日，江苏省教育网信办通报的网络安全事件的复现，该事件对我校带来严重不良影响。

经调查，该事件的复现原因是：libwx.njtech.edu.cn 系统升级重装，系统配置参数被重置为默认值，工程师未按

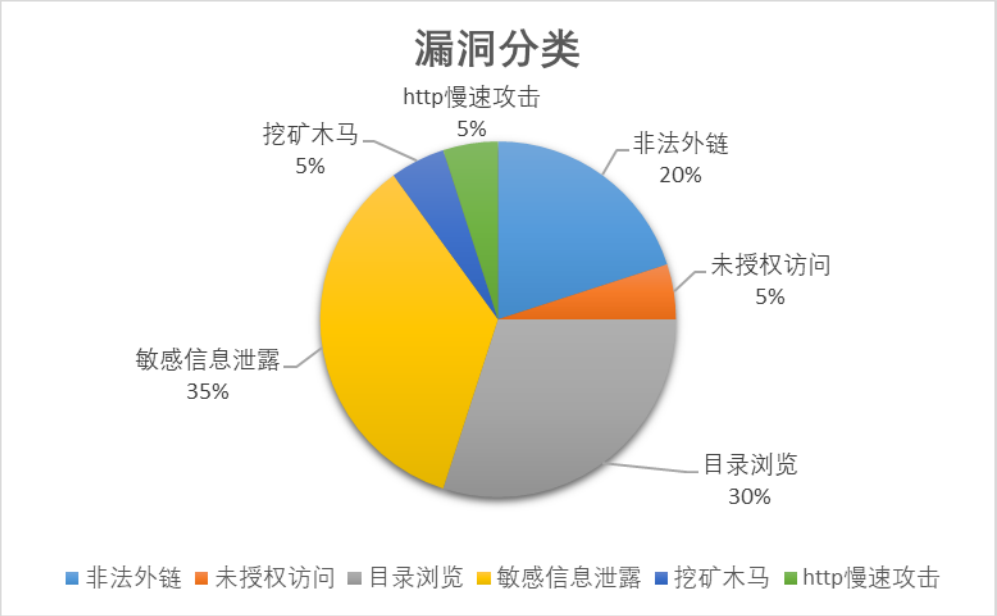
照规范将之前的漏洞加固修复，导致漏洞重复出现。

网络安全事件复现的危害和后果：网络安全事件复现会导致该系统存在被攻击的可能性，对我校网络安全环境造成严重威胁，上级主管部门将对复现情况进行全省通报，直接影响到我校在全省教育系统网络安全责任考核中的成绩。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 20 个。其中非法外链 4 个，未授权访问 1 个，目录浏览 6 个，敏感信息泄露 7 个，挖矿木马 1 个，http 慢速攻击 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 10 月共发现漏洞 20 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
附件存在身份证信息泄露	加强防范意识，附件中去除或脱敏身份证信息。
挖矿木马病毒	定期维护个人电脑，更新杀毒软件版本，定期对电脑进行杀毒扫描。参考 9 月份网络安全月报提示。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，各单位（部门）响应处理及时，未造成网络安全事件。但设备感染挖矿病毒问题依然非常严重，各单位（部门）应提醒本单位（部门）师生员工要定期关注个人设备运行状况，做好宣传教育，严厉打击虚拟货币“挖矿”行为。各单位（部门）应对本单位（部门）被通报的网络安全事件高度重视，压实责任、及时整改、加强管理，杜绝网络安全事件复现，共同维护校园网络安全。

网络与信息系统安全联系电话：58139275。

信息管理中心

2021 年 11 月 3 日