2021 年网络与信息系统安全月报
（9 月）

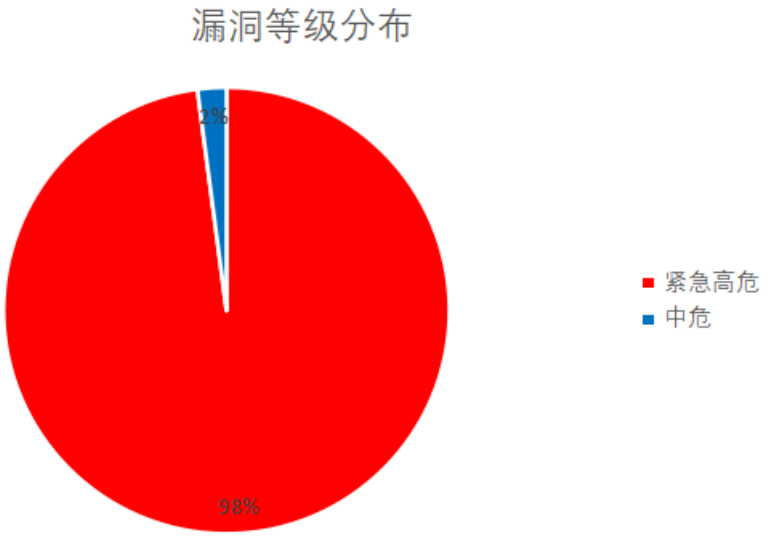
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 9 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 48 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 46 个，校外通报漏洞 2 个。其中紧急高危 47 个，中危漏洞 1 个，低危漏洞 0 个，紧急高危占比：98%。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：江苏省教育网信办，补天漏洞平台。

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	10.7.12.12;10.3.89.4;10.3.89.30	木马-挖矿木马	已修复	个人和计算机科学与技术学院机房
补天漏洞平台	202.119.243.119	逻辑漏洞	已修复	科学研究院

表一：第三方通报漏洞

(三)非法外链情况

本月检查到 12 家单位所属网站共出现 26 次非法外链，具体 12 家单位情况如下：

网站（系统）	部门
http://trans.njtech.edu.cn/	交通运输工程学院
http://2011.njtech.edu.cn/	国家“江苏先进生物与化学制造”协同创新中心
http://maker.njtech.edu.cn/	教务处

http://nthy.njtech.edu.cn/	化工学院
http://glp.njtech.edu.cn/	江苏省药物研究所有限公司
http://tyxy.njtech.edu.cn/	体育学院
https://safety.njtech.edu.cn/	保卫处
http://pharm.njtech.edu.cn/	药学院
http://cce.njtech.edu.cn/	土木学院
http://spy.njtech.edu.cn/	食品与轻工学院
http://gra.njtech.edu.cn/	研究生院
http://sp.njtech.edu.cn/	大学科技园管理办公室

表二：非法外链汇总表

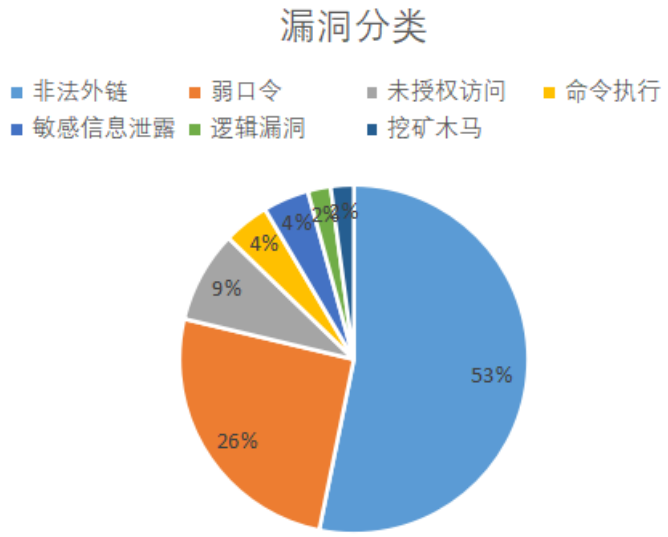
(四)挖矿病毒专项检查

本月，信息管理中心组织力量对我校终端及服务器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电脑终端及服务器共 80 个。信息管理中心对这些受感染设备进行了紧急网络隔离，并通知设备所属单位及个人，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，确保校内电脑终端及服务器正常运行。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 48 个。其中非法外链 26 个，弱口令 12 个，未授权访问 4 个，命令执行 2 个，敏感信息泄露 2 个，逻辑漏洞 1 个，挖矿木马 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 9 月共发现漏洞 48 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
弱口令数量较多	加大运维管理员口令安全意识，定期检查系统密码复杂度。
非法外链较多	加强扫描力度，定期处理过期公告，网页使用链接应为官方网站，不采用临时网站。尽量不在学校网站中添加非学校域名的网站链接。

（二） 挖矿病毒威胁风险与防范

1、**“挖矿”木马的定义：**不法分子将木马程序植入到他人的计算机中，在受害者不知情的情况下，中毒设备自动“挖矿”，使多台计算机资源帮助不法分子获得虚拟货币；这样的木马程序就是“挖矿”木马病毒。

2、**“挖矿”病毒对电脑的影响：**一般计算机中了“挖矿”木马之后会有以下表现：网络流量很大，耗电量急剧上升，运行速度变慢，显卡占用比很高，网络安全隐患，性能明显降低。

3、**“挖矿”木马查杀方法：**

1)备份已知的重要文件，并重装系统；

2）联系信息管理中心58139277，我们会帮助您处理相关问题。

4、**电脑病毒的防范：**

1)不随便点开来历不明的邮件链接；

2)对个人上网账号和密码信息保密；

3)避免使用弱口令，比如密码设置为123456或生日，姓名拼音等等；

4)不使用没有经过病毒查杀的移动硬盘；

5)使用正版软件，校内用户可以在**我校软件正版化平台**：https://soft.njtech.edu.cn/ 或者**开源镜像站** https://mirrors.njtech.edu.cn/，下载需要的软件。

四、网信安全每月小结

本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。但本月发现一些长期强调的网络安全问题，如弱口令，非法外链漏洞仍然较多，多个学院

机房服务器和个人电脑感染挖矿病毒，对正常科研、教学及学校关键信息系统（网站）正常运行造成很大安全隐患，需要重点关注，并积极排查整改，维护正常网络环境。

网络与信息系统安全联系电话：58139275。

信息管理中心

2021 年 10 月 5 日