2022 年网络与信息系统安全月报

（9 月）

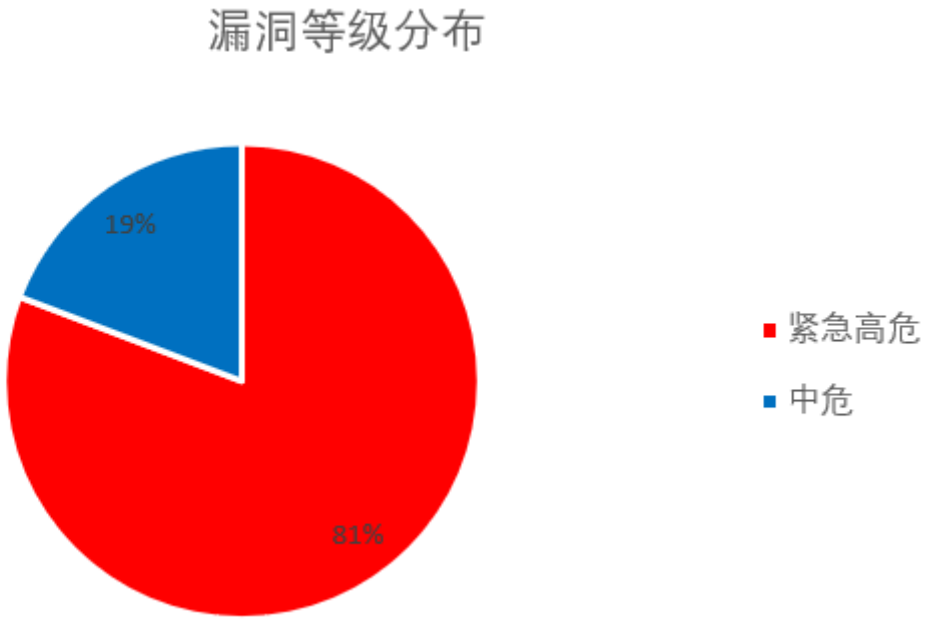
各单位、部门：

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 26 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 20 个，校外通报漏洞 6 个。其中紧急高危 21 个，中危漏洞 5 个，低危漏洞 0 个，紧急高危占比：80.7%。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	202.119.248.147	目录遍历	已修复	化工学院
教育 SRC	202.119.248.147	文件上传	已修复	化工学院
教育 SRC	202.119.248.143	目录遍历	已修复	安全科学与工程学院
教育 SRC	202.119.248.143	文件上传	已修复	安全科学与工程学院
教育 SRC	202.119.248.143	信息泄露	已修复	安全科学与工程学院
教育 SRC	202.119.248.143	越权访问	已修复	安全科学与工程学院

(三)非法外链情况

本月检查到 8 家单位所属网站共出现 11 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://cise.njtech.edu.cn/	计算机科学与技术学院	1 次
http://kyy.njtech.edu.cn/	科学研究院	2 次
http://tw.njtech.edu.cn/	团委	3 次
http://art.njtech.edu.cn/	艺术设计学院	1 次

http://mech.njtech.edu.cn/	机械与动力工程学院	1 次
http://2011.njtech.edu.cn/	2011 学院	1 次
http://english.njtech.edu.cn/	外国语言文学学院	1 次
http://jkjy.njtech.edu.cn/	后勤保障处	1 次

（四）网络攻防应急演练。

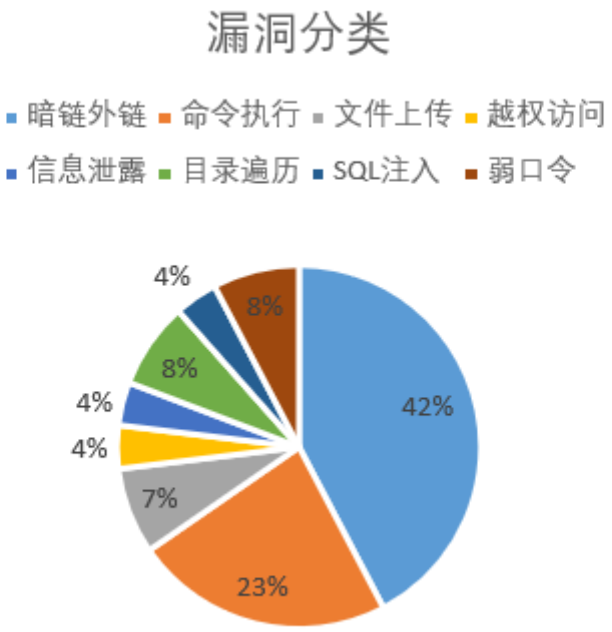
9 月 28 日，在学校第三季度网络安全工作会议暨校内网络攻防应急演练中，共发现 7 个系统存在严重安全隐患，具体情况如下：

系统名称	访问地址	部门	漏洞类型	造成危害
南京工业大学分析测试中心	http://202.119.249.17:8080	材料化学工程国家重点实验室	向日葵命令执行	页面篡改/信息泄露
南京工业大学教室节电控制管理系统	http://202.119.249.104:8014	后勤保障处	SQL 注入攻击	信息泄露
教室智慧系统	http://202.119.249.16	材料科学与工程学院	shiro 命令执行	页面篡改/信息泄露
宝和数据-科技查新系统	http://202.119.252.181:9000	图书馆	fastcgi 命令执行	获取服务器权限
三维虚拟仿真平台	http://202.119.249.57:8090	化学与分子工程学院	shiro 命令执行	页面篡改/信息泄露
国家虚拟仿真实验教学项目	http://202.119.248.147	化工学院	shiro 命令执行	页面篡改/信息泄露
本科教学管理与服务平台	https://jwgl.njtech.edu.cn	教务处	0day 命令执行	帆软漏洞(双非系统)

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 26 个。其中暗链外链 11 个，命令执行 6 个，文件上传 2 个，越权访问 1 个，信息泄露 1 个，目录遍历 2 个，SQL 注入 1 个，弱口令 2 个。漏洞分类占比如下图：



(二)漏洞修复情况

2022 年 9 月共发现漏洞 26 个，本月漏洞均已修复。

三、安全威胁风险与防范

为提升学校网络安全威胁的防范能力，9 月对学校的关键信息资产进行了威胁风险与防范升级，具体工作内容有：

1、 智慧南工统一身份验证加固。

2、 VPN 平台升级，增加双因子验证。

3、 合作厂家使用 SSL 登录账号全面梳理。

4、 智慧南工数据中台安全策略加固。

5、 各平台厂家签署系统安全承诺书及保障方案。

6、 完善网络边界访问控制。

在本月信息系统安全检测中发现，主要存在以下安全威胁风险。

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。
服务器安装远程工具	清查自身管理服务器，禁止安装向日葵等远程登录工具。
系统存在弱口令	定期修改弱口令，加强弱口令安全意识。
系统版本存在高危漏洞	定期针对系统做漏洞扫描，安装软件版本确认无问题在安装。

四、网络安全宣传周活动

根据教育部思想政治工作司《关于组织开展2022年国家网络安全宣传周校园日活动的通知》、中共江苏省委网信办《2022 年江苏省网络安全宣传周活动实施方案》和江苏省教育厅办公室《关于开展2022年江苏省教育系统网络安全宣传周校园日活动的通知》，发布了南京工业大学《关于开展 2022 年网络安全宣传周校园日系列活动的通知》，开展了网络安全宣传周的相关活动，具体工作内容如下：

（一）校园日在线直播活动

参加教育部和我省教育系统网络安全宣传周校园日重点活动。

1、 观看由教育部思想政治工作司和公安部刑事侦查局共同打造的一堂面向全国师生的网络安全公开课。

2、 全校研究生、本科生通过“中国大学生在线”微信公众号的“守护青春”栏目参与“守护青春、网络有你”全国大学生网络安全知识答题活动。

3、 师生通过中国大学生在线官网（dxs.moe.gov.cn）进入“守护青春、网络有你”网络安全知识学习专区，加强理性看待媒介信息、信息甄别和正确使用传播媒介等方面知识的学习。

4、 2022 年 9 月 6 日 15:00，各单位各部门组织师生在线观看我省教育系统网络安全宣传周校园日在线直播活动。

（二）网络安全攻防演练

为进一步健全我校网络安全事件应急工作机制，规范网络安全事件处置工作流程，检验《南京工业大学校园网络与信息安全应急处置预案》的有效性，验证各单应对网络和信息安全突发事件的组织指挥能力和应急处置能力，学校发布了《关于开展网络安全应急演练的通知》（南工信〔2022〕1 号），根据通知精神和要求，在 9 月 19 日至 9 月 28 日开展了全校网络安全应急演练。

在本次演练中，大部分部门由于熟练掌握一键断网处置以及应急处置流程，能在信息管理中心发出安全预警后，及时进行一键断网，并及时修复了漏洞。但是托管在校外的“双非系统”无法进行一键断网，各部门要加强对本单位“双非系统”的排查，形成相应的应急响应机制。

此次演练寓“演”于“练”，以“练”为主，突出实战，进一步建立健全了我校网络安全应急工作机制，提升各部门的网络安全意识，检验各单位对网络安全事件的应急处置能力和防范信息系统风险的能力，落实和完善网络安全应急预案，建立了统一指挥、协调有序的应急管理机制和协调机制。

(三) 钓鱼邮件演练

在国家网络安全宣传周期间，我校在 9 月 12 日至 9 月 14 日期间组织开展了钓鱼邮件演练。本次演练共向全校师生发送模拟钓鱼邮件 46000 余封，共有 2039 名师生阅读了钓鱼邮件，其中有 916 名师生点击了可疑链接，585 名师生在假的登录页面输入用户账号和密码。

在本次演习中，大部分师生看穿了钓鱼邮件的“伪装”，并积极地向信息管理中心反馈和举报，还有师生准备对服务器发起反攻，充分体现了我校师生良好的网络安全意识。通过本次钓鱼演练，让广大师生切实体会到钓鱼邮件的迷惑性和隐蔽性，提升了师生的网络安全意识。

（四）网络安全在线知识竞赛

9 月 23 日 9 点-9 月 27 日 9 点，我校通过南京工业大学在线考试平台，组织开展了“争做校园好网民，凝聚网络正能量，青春献礼二十大”主题网络安全在线知识竞赛。本次竞赛以网络安全法律法规、网络安全基础知识、个人信息保护等内容为主。

本次竞赛分教师组和学生组。全校共有近 2000 名师生参加，教师组来自党委办公室的狄远帆与团委的花冬进老师以 94 分的成绩，最快完成了比赛，获得了教师组一等奖。学生组来自建筑学院的陈子卿和徐永旺同学，测绘科学与技术学院的包煜同学以 98 的成绩，最快完成了比赛，获得了学生组一等奖。

（五）网络反诈骗活动

为持续做好防范电信网络诈骗宣传教育工作，全面提升全校师生防范电信网络诈骗的意识和能力,从 9 月 26 日至 9 月 30 日,学校联手中国电信南京浦口区分公司在全校范围内开展“电信诈骗,你我共防”活动。

本次活动中，通过反电信网络诈骗宣传展、发放宣传手册、在“南工在线”和 B 站反电信网络诈骗设立宣传专栏、反电信网络诈骗知识竞赛等多种形式开展网络反诈骗活动。

通过活动，广大师生了解了电信网络诈骗的危害和主要手段、树立安全意识，养成了良好的个人信息保护习惯、提高了识别和防范电信网络诈骗能力。

五、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。但我校部分信息系统（网站）存在命令执行、文件上传、弱口令等高危漏洞，威胁服务器安全。部分单位相关负责人存在网络安全意识淡薄，一键断网流程不熟悉等问题。

各单位要加强重点信息系统（网站）网络安全应急措施落实，规定动作务必做到位，常态化巡检不可少，完善应急预案，做好应急准备。以“小辛苦”换取“大稳定”，守护我校网络安全稳定。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 10 月 14 日