2022 年网络与信息系统安全月报

（3 月）

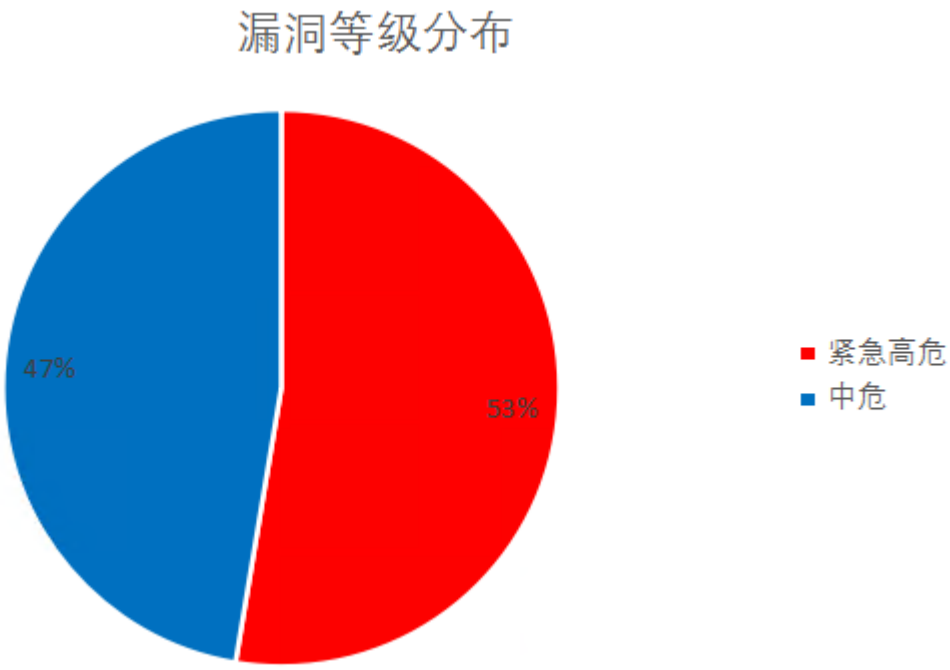
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 3 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 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 9 个，校外通报漏洞 10 个。其中紧急高危 10 个，中危漏洞 9 个，低危漏洞 0 个，紧急高危占比：53%。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、教育部 APP 安全通报平台。

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	58.213.118.181	感染木马	已修复	大学科研园管理办公室
江苏省教育网信办	218.94.124.46	感染病毒木马	已修复	个人电脑
江苏省教育网信办	http://gra.njtech.edu.cn/	身份证泄露	已修复	研究生院
江苏省教育网信办	南京工业大学数据泄露	信息泄露	已修复	教师，科学研究院
江苏省教育网信办	http://gra.njtech.edu.cn/	身份证泄露	已修复	研究生院
教育部 APP 安全通	i 南工 APP	软件漏洞	已修复	信息管理中心

报平台				
教育 SRC	http://zrb.njtech.edu.cn/	文件下载	已修复	学术期刊编辑部
教育 SRC	http://skb.njtech.edu.cn/	文件下载	已修复	学术期刊编辑部
教育 SRC	http://green.njtech.edu.cn	弱口令	已修复	计算机科学与技术学院
教育 SRC	http://green.njtech.edu.cn	配置文件泄露	已修复	计算机科学与技术学院

(三)非法外链情况

本月检查到 1 家单位所属网站出现 1 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://jgy.njtech.edu.cn/	经济与管理学院	1 个

(四)网络安全应急演练

本月，信息管理中心对全校网络信息系统组织开展了网络安全应急演练。对校内在线使用的 900 多个信息资产，使用扫描器进行漏洞和弱口令扫描，根据扫描结果排查可利用的高危漏洞。确定以下三个系统作为演练对象：

1．后勤保障处的校医院系统（http://202.119.248.35/）：该系统存在弱口令和命令执行漏洞，网络安全工程师利用系统漏洞添加服务器登录账号，篡改页面。半个小时内未接到系统责任部门反馈。随后信息管理中心提供漏洞报告给系统责任部门，由系统责任部门通知厂商停止网站服务，并修复漏洞。

2. 化学与分子工程学院的实验教学智能管理系统（http://202.119.249.57:88）：该系统存在弱口令漏洞，但系统管理员在巡查时发现后台存在入侵记录，及时关闭系统，防止了系统被攻破。

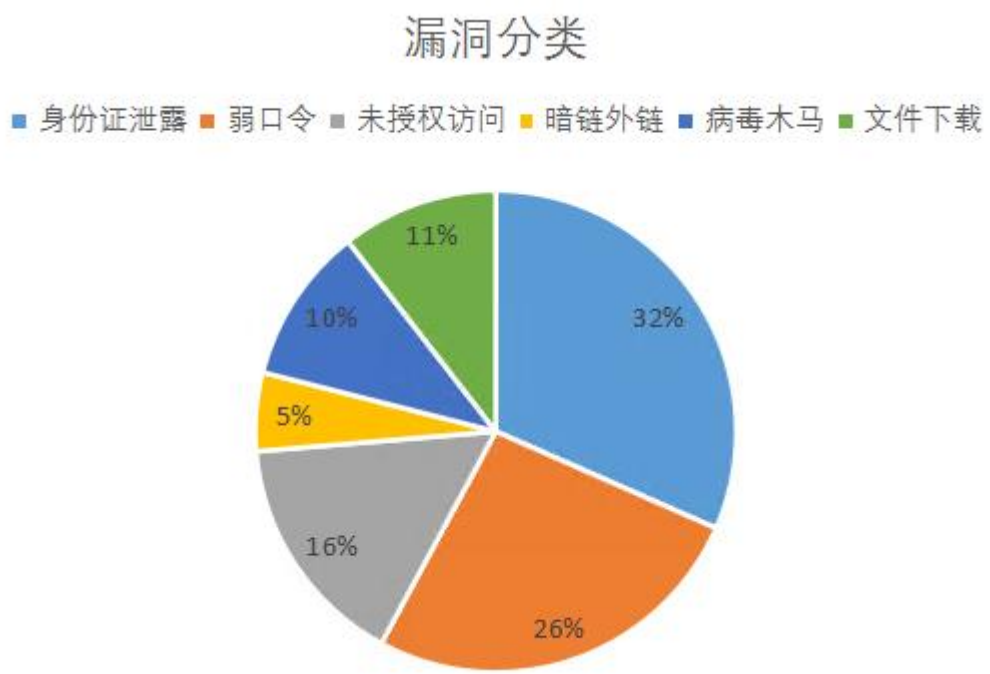
3. 后勤保障处的厚学楼教室节能控制系统（http://202.119.249.104）：该系统存在 SQL 注入漏洞，但系统管理员在服务器中安装了防火墙软件，出现 SQL 注入漏洞无法利用，攻击行为被阻断，系统无法被入侵。

网络安全应急演练从实战出发，现场演示网站系统存在漏洞的应急防御处置办法，达到了增强网络安全应急处置能力，锻炼网络安全应急工作队伍，完善网络安全应急预案体系，全面提高网络安全应急水平的目的。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 19 个。其中身份证泄露 6 个，弱口令 5 个，未授权访问 3 个，暗链外链 1 个，病毒木马 2 个，文件下载 2 个。漏洞分类占比如下图：



(二)漏洞修复情况

2022 年 3 月共发现漏洞 19 个，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
网页存在信息泄露	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。
登录默认弱口令较多	普及安全意识，做好密码保护工作，修改开发厂家和运维人员的默认密码。
部分网站存在未授权端口	梳理网站开放的所有端口，非白名单端口需提供必需开放说明，关闭不必要对外开放端口

（二）个人电脑病毒威胁防范

个人电脑日常使用防毒注意事项：

1. 关闭或删除系统中不需要的服务。默认情况下，许多操作系统会安装一些辅助服务，如 FTP 客户端、Telnet 和 Web 服务器。这些服务为攻击者提供了方便，而对用户又没有太大用处。如果删除或者关闭这些服务，就能大大减少被攻击的可能性。

2. 建立安全上网习惯。例如：对一些来历不明的邮件及附件不要打开，不要上一些不太了解的网站、不要执行从 Internet 下载后未经杀毒处理的软件等，这些良好习惯会使您的计算机更安全。

3. 经常升级安全补丁。据统计，有 80%的网络病毒是通过系统安全漏洞进行传播的，所以我们应该定期安装最新的安全补丁，防范病毒感染。

4. 使用复杂密码。有许多网络病毒就是通过猜测简单密码的方式攻击系统的，因此使用复杂的密码，将会大大提高计算机的安全系数。

四、网信安全每月小结

本月我校信息系统漏洞总量较少，因各部门响应处理及时，未造成网络安全事件。但信息泄露和病毒感染问题时有发生，各单位应在上传附件时，须仔细检查文件是否存在敏感信息，对例如身份信息、地址信息等敏感信息，及时进行模糊化处理。各单位要高度认识网络安全的极端重要性，宣传普及网络病毒知识和安全防范技巧，紧绷安全之弦，提高师生网络安全意识。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 4 月 8 日