

2022 年网络与信息系统安全月报 (12 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 12 月份网络与信息系统安全通报如下：

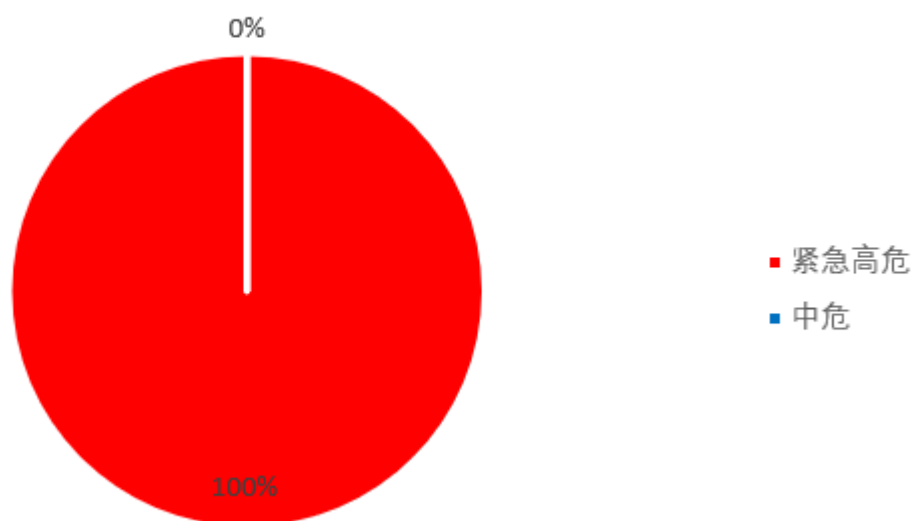
一、本月整体安全情况

(一)漏洞发现情况

本月共发现漏洞 6 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 6 个，校外通报漏洞 0 个。其中紧急高危 6 个，中危漏洞 0 个，低危漏洞 0 个，紧急高危占比：100%。

紧急、高危、中危、低危漏洞统计情况见下图：

漏洞等级分布



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

本月未收到第三方漏洞通报。

(三) 非法外链情况

本月检查到 3 家单位所属网站共出现 3 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://cqt.njtech.edu.cn/	党委宣传部	1 次	通信管理局
http://chem.njtech.edu.cn/	化学与分子工程学院	1 次	通信管理局
http://zwc.njtech.edu.cn/	后勤保障处	1 次	校内自查

(四) 出台网络安全预警与监测办法

为进一步加强网络安全监测预警和信息通报工作，有效防范网络安全事件的发生，维护学校网络安全，学校本月制定了《南

京工业大学网络安全监测预警和信息通报实施办法》。办法从四个方面建立健全我校监测预警和信息通报机制，对风险进行预警，做到“早发现、早报告、早处置”，减少和防止不良信息的传播，确保信息网络的畅通和安全。

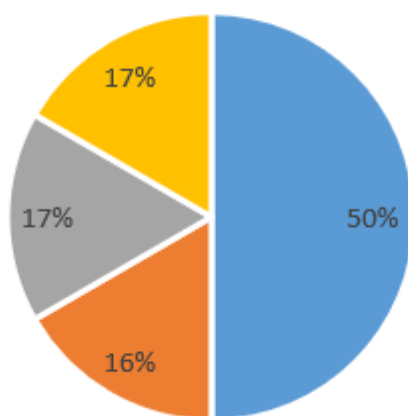
二、本月整体安全情况

(一)漏洞类型统计

本月共发现漏洞6个。其中暗链外链3个，信息泄露1个，弱口令1个，文件上传1个。漏洞分类占比如下图：

漏洞分类

■ 暗链外链 ■ 文件上传 ■ 弱口令 ■ 信息泄露



(二)漏洞类型统计

本月共发现漏洞6个，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
附件存在身份证泄露	发布新闻公告中附件禁止包含或

	脱敏身份证等敏感信息。
网站存在文件上传高危漏洞	对外服务系统需提前检测是否存在漏洞，及时修复避免发生安全隐患。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，因各部门响应处理及时，未造成网络安全事件。寒假期间，各单位应加强坚持问题导向、底线思维，突出以防为主、防治结合，以“时时放心不下”的责任感，狠抓网络安全责任落实，全面排查整治各类网络安全隐患，要高度重视对所属信息系统和网站的安全监管。加大假期信息系统和网站巡查力度，严防发生各类网络安全事件。加强对师生的网络安全教育，重点加强防传销诈骗、防钓鱼邮件、防计算机病毒等方面教育，全面提高师生的网络安全意识和自我防护能力。

网络与信息系统安全联系电话：58139275。

信息管理中心

2023年1月9日