2022 年网络与信息系统安全月报

（1 月）

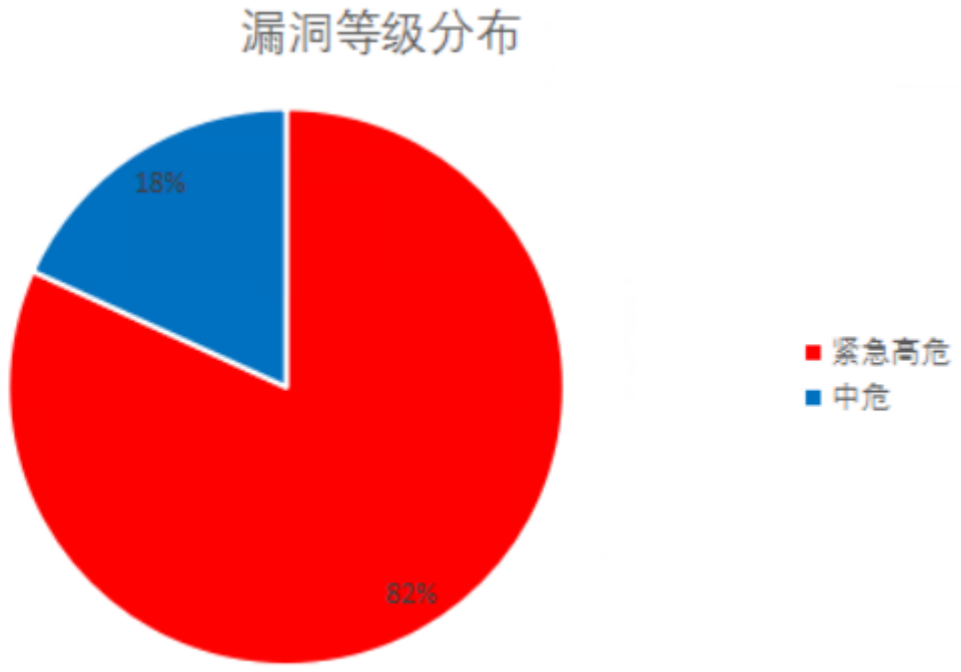
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 1 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 11 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 8 个，校外通报漏洞 3 个。其中紧急高危 9 个，中危漏洞 2 个，低危漏洞 0 个，紧急高危占比：82%。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。

漏洞通报的来源为教育 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	https://jfpt.njtech.edu.cn/	登录默认口令	已修复	财务处
教育 SRC	http://sycl.njtech.edu.cn/	命令执行	已修复	实验室建设与管理处
教育 SRC	https://jwgl.njtech.edu.cn/	登录默认口令	已修复	教务处

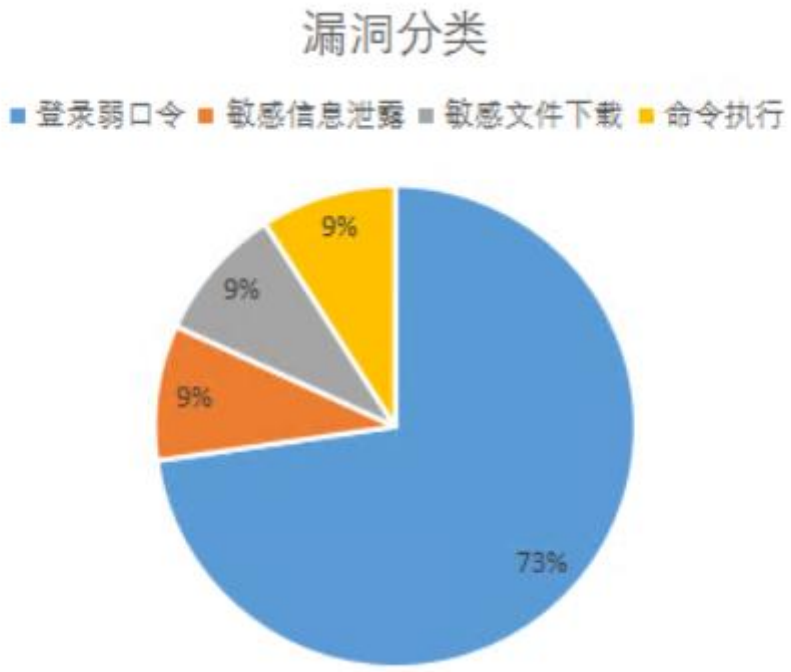
(三)非法外链情况

本月未检测到我校网站存在暗链外链情况。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 11 个。其中登录弱口令 8 个，敏感信息泄露 1 个，敏感文件下载 1 个，命令执行 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2022 年 1 月共发现漏洞 11 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
网页存在身份信息泄露	发布网页的附件中禁止填写身份证信息，如必须填写，必须将出生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。
敏感文件下载	服务器禁止在访问目录下备份网站压缩文件

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。本月我校暗链外链威胁状况明显改善，但新型网络安全问题需要高度重视，个人终端及服务器感染“肉鸡病毒”和“挖矿病毒”现象时有发生，严重威胁校园科研、教学等关键信息系统（网站）正常运行，各单位需要持续关注，加大宣传教育力度，普及健康

的互联网使用习惯，共同维护校园网络安全环境。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 2 月 21 日