2022年网络与信息系统安全月报

（8月）

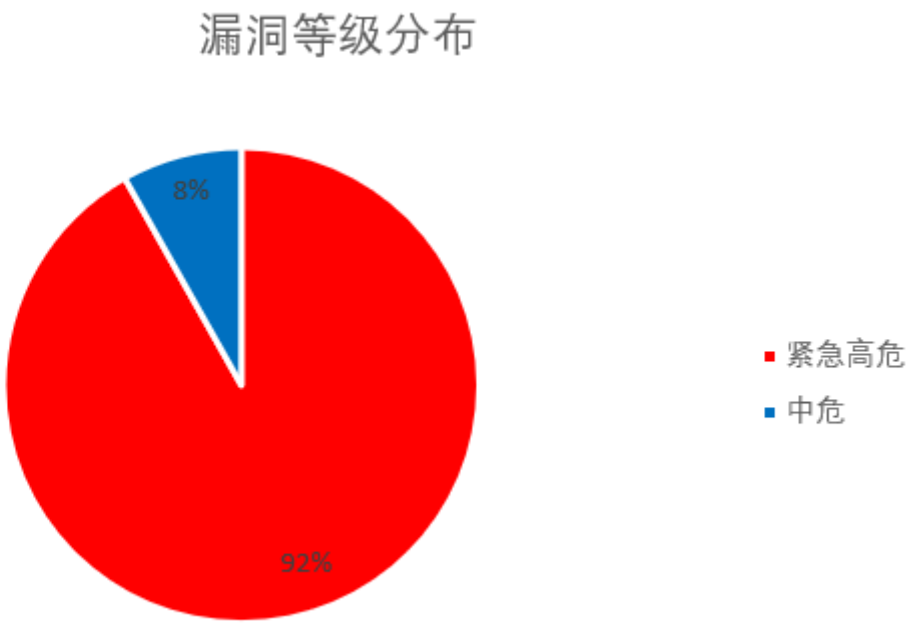
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将8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

本月共发现漏洞49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洞43个，校外通报漏洞6个。其中紧急高危45个，中危漏洞4个，低危漏洞0个，紧急高危占比：91.8%。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、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
教育 SRC	202.119.248.147	验证码爆破	已修复	化工学院
教育 SRC	202.119.248.147	逻辑越权	已修复	化工学院
教育 SRC	202.119.248.147	Shiro 命令执行	已修复	化工学院
教育 SRC	http://202.119.249.142:9001/	弱口令	已修复	保卫处
教育 SRC	202.119.249.129	跨站脚本	已修复	教务处
补天漏洞平台	https://store.njtech.edu.cn/	服务端请求伪造	已修复	信息管理中心

(三)非法外链情况

本月检查到 6 家单位所属网站共出现 38 次非法外链，具体情况如下：

网站（系统）	部门	频次
http://tyxy.njtech.edu.cn/	体育学院	2 次
http://202.119.243.15	教务处	1 次
http://cise.njtech.edu.cn/	计算机科学与技术学院	1 次
http://dgy.njtech.edu.cn/	电光源材料研究所	32 次
http://english.njtech.edu.cn/	外国语言文学学院	1 次
http://2011.njtech.edu.cn/	2011 学院	1 次

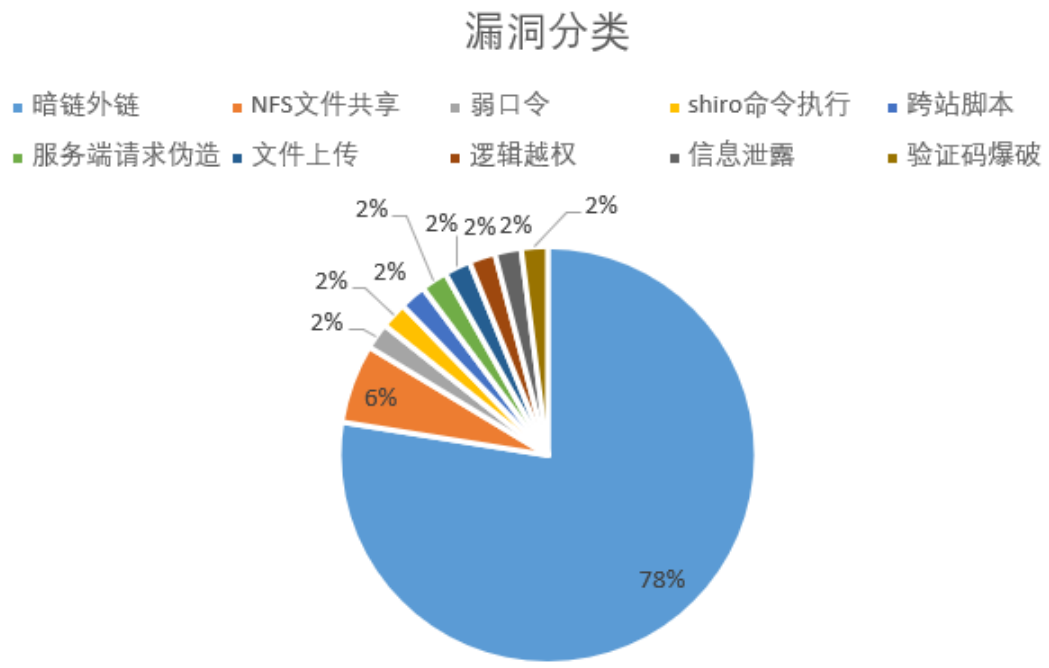
（四）开展数据安全情况调查

本月，我校根据工作需要，继续进行数据安全风险隐患排查，积极落实网络数据管理，摸查校内信息系统服务器操作系统环境，对网络数据进行全生命周期安全管理，做好校内师生个人数据保护。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 49 个。其中暗链外链 38 个，NFS 文件共享 3 个，弱口令 1 个，shiro 命令执行 1 个，跨站脚本 1 个，服务端请求伪造 1 个，文件上传 1 个，逻辑越权 1 个，信息泄露 1 个，验证码爆破 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

本月发现的漏洞均已修复。

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。
敏感数据对外共享	清查自身服务对外协议，将非必要对外开放协议限制到本地访问。
系统存在弱口令	定期修改弱口令，加强弱口令安全意识。
系统版本升级造成高危漏洞	升级完系统或软件及时针对服务器或网站进行漏洞，确保无漏洞。

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。本月漏洞危害等级较高，存在命令执行、

跨站脚本、弱口令等高危漏洞，同时，网页暗链外链问题依旧严峻。请各部门加强网页安全管理，落实安全管理职责，做好风险防控，要求系统开发及运维方做好安全巡检，及时发现安全隐患，处置安全漏洞，打好系统补丁，确保信息系统持续安全稳定，以实际行动迎接党的二十大胜利召开。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 9 月 8 日