2020 年网络与信息系统安全月报

（10 月）

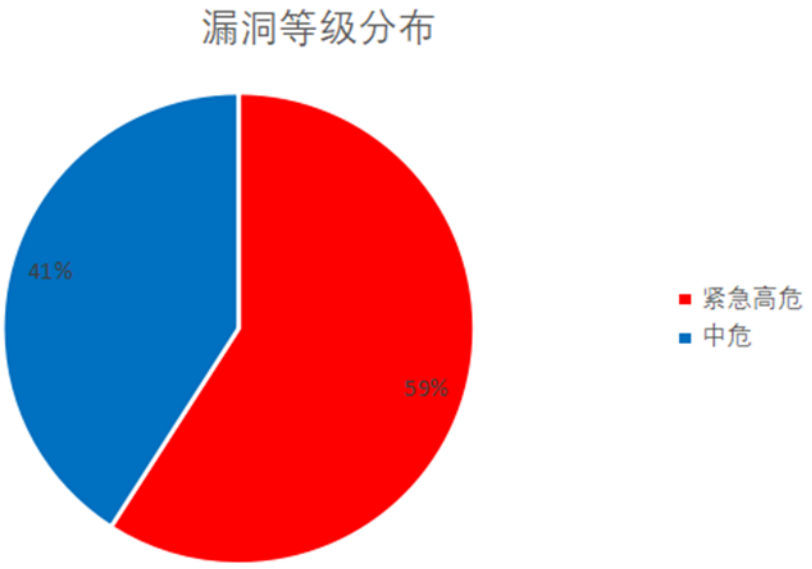
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 10 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

本月通过在校内网站监测、人工挖掘以及安全专项检查自测发现漏洞 22 个，校外通报漏洞 0 个。其中紧急高危 13 个，中危漏洞 9 个，低危漏洞 0 个，紧急高危占比：59%。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。

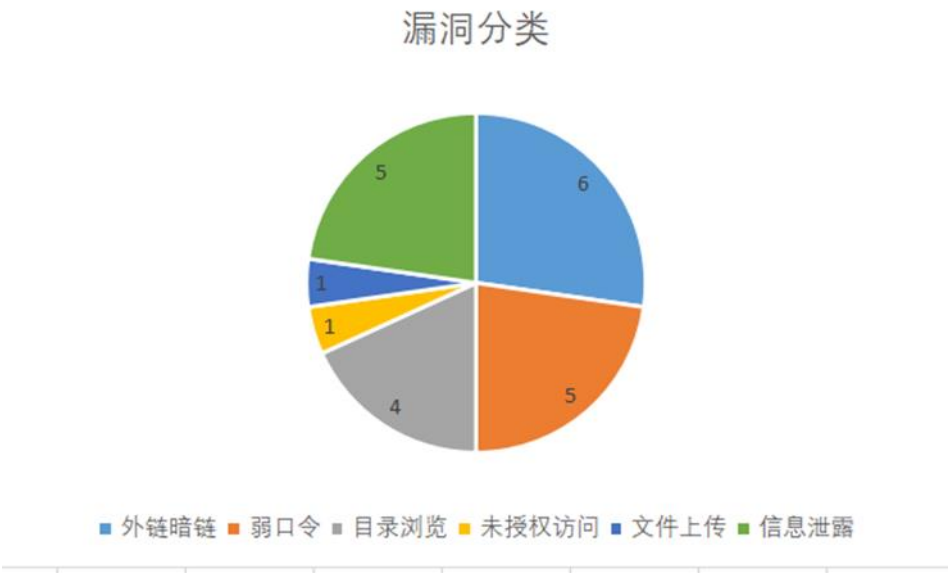
(二)漏洞通报情况

学校 10 月份未收到教育部通告漏洞，未接收到其他第三方漏洞平台通报，本月态势良好。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 22 个。其中外链暗链 6 个，ftp 弱口令 3 个，web 弱口令 2 个，目标浏览 4 个，未授权访问 1 个，任意文件上传 1 个，其他类漏洞 5 个。漏洞分类占比如下图：

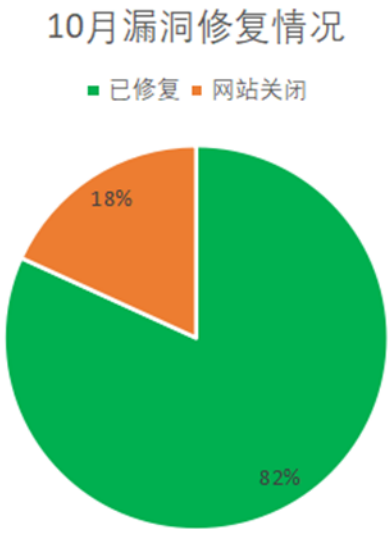


(二)漏洞修复情况

2020 年 10 月共发现漏洞 22 个。其中按时修复漏洞的有 20 个，因为漏洞无法修复，通过关停系统避免漏洞造成次生危害的漏洞有 2 个（见表一），具体情况如下：

域名（IP 地址）	风险等级	漏洞类型	系统名称	使用部门
http://president.njtech.edu.cn	高危	外链暗链	黄维院士网站	政策研究与规划处
http://202.119.243.44/	中危	tomcat 默认安装文件未删除	后勤平台	后勤保障处

表一：关停系统汇总表



三、安全威胁风险与防范

安全威胁风险	防范措施建议
服务器长时间未更新补丁，出现微软系统漏洞	及时针对服务器进行补丁升级。
web 后台仍存在弱口令	系统管理员定期修改密码，密码必须为强密码。
外网攻击影响校内部分系统正常运行	重要数据中心需有防火墙防御，对外开放系统需有 waf 防御。
部分服务器存在 445 端口服务	针对设备做端口策略限制

四、网信安全每月小结

本月我校信息系统漏洞数与上月相比有显著下降，因各部门响应处理及时，未造成网络安全事件。各单位应继续坚决守好网络信息安全的红线，定期对本单位信息系统进行梳理，并及时上报，明确各信息系统直接责任人，提高网络安全防范意识。

网络与信息系统安全联系电话：58139275,83172363。

信息服务部

2020 年 11 月 3 日