2020 年网络与信息系统安全月报

（9 月）

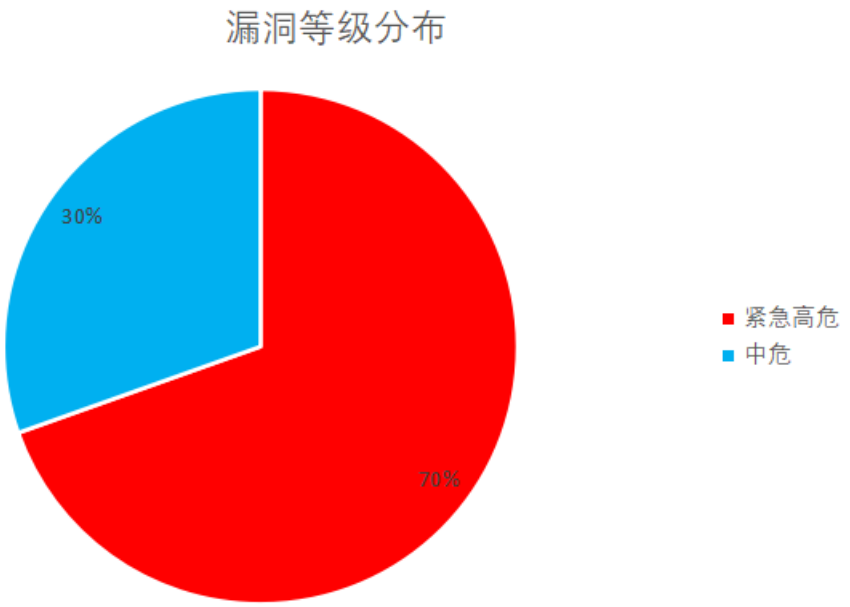
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 9 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 46 个，校外通报漏洞 0 个。其中紧急高危 32 个，中危漏洞 14 个，低危漏洞 0 个，紧急高危占比：70%。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。

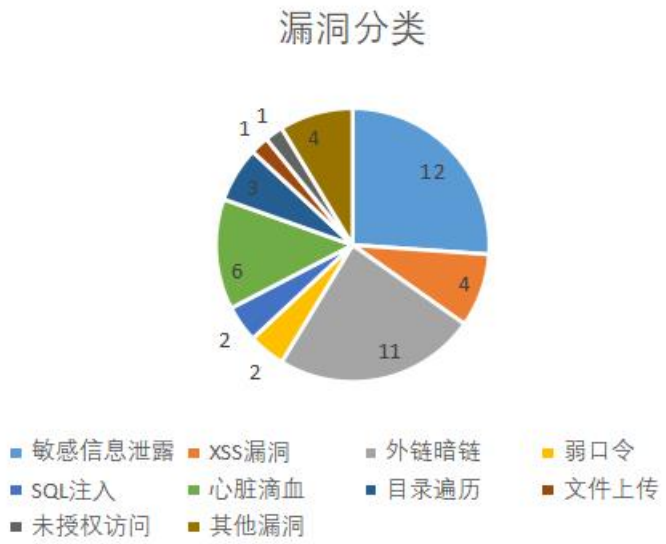
(二)漏洞通报情况

学校 9 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

本月通过自测共发现漏洞 46 个，外部通报漏洞 0 个。其中敏感信息泄露 12 个，外链暗链 11 个，XSS 漏洞 4 个，弱口令 2 个，SQL 注入 2 个，心脏滴血 6 个，目录遍历 3 个，文件上传 1 个，未授权访问 1 个，其他类漏洞 4 个。漏洞分类占比如下图：

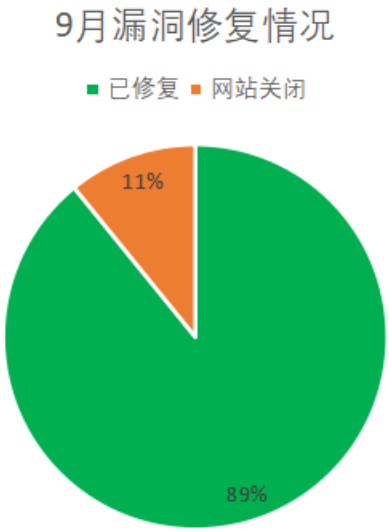


(二)漏洞修复情况

2020 年 9 月共发现漏洞 46 个。其中按时修复漏洞的有 41 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 5 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://202.119.249.14/	高危	跨站脚本 XSS	自主学习学分管理系统	教学事务部
http://202.119.249.14/	高危	目录遍历	自主学习学分管理系统	教学事务部
http://10.21.254.10/	高危	弱口令	监控摄像头	后勤保障处
http://ztb.njtech.edu.cn/	高危	后台存储型 XSS	招投标管理系统	国有资产管理处
http://ztb.njtech.edu.cn/	高危	文件上传	招投标管理系统	国有资产管理处

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
部分网站将初始密码更新在网页上	删除初始密码通知，以短信方式获取密码，新增强制改密码措施。
部分网站所挂外链域名失效，被其他恶意抢注	定期检查外链是否过期被其他抢注，定期清理失效的外链。
部分服务器软件未升级导致漏洞	扫描服务器漏洞并针对性升级

四、网信安全每月小结

本月我校信息系统漏洞总数量环比下降了 28%，因各部门响应处理及时，未造成网络安全事件。在本月，通过学习贯彻校网信安全会议精神，结合全国网络安全宣传周的大力宣传，全校上下网信安全意识进一步提升，网络安全责任网进一步织密。

网络与信息系统安全联系电话：58139275,83172363。

信息服务部

2020 年 10 月 12 日