2020 年网络与信息系统安全月报

(11 月)

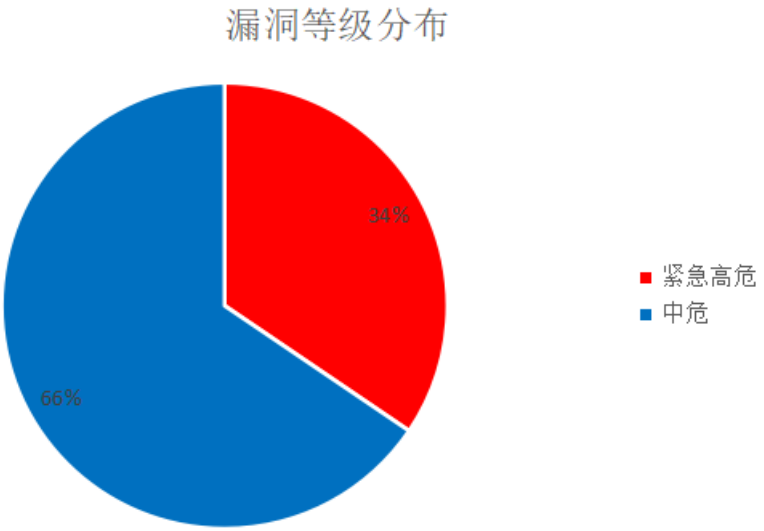
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 11 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 30 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 21 个，校外通报漏洞 9 个。其中紧急高危 10 个，中危漏洞 20 个，低危漏洞 0 个，紧急高危占比：34%。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

我校 11 月份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。

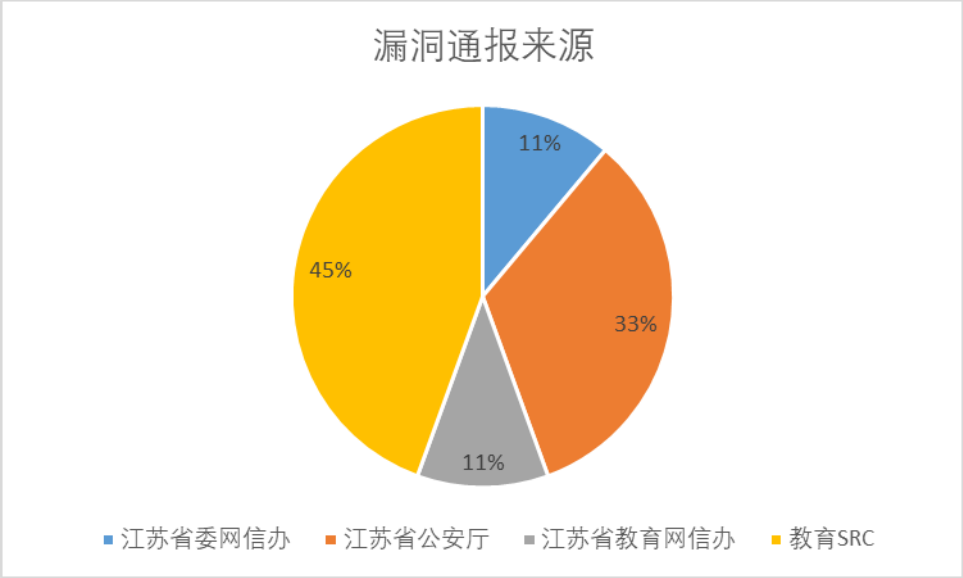
漏洞通报的来源包括：江苏省省委网信办、江苏省公安厅、江苏省教育网信办、教育 SRC 等。具体情况如下：

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
江苏省委网信办	ihed.njtech.edu.cn	敏感信息泄露	已修复	政策研究与规划处
江苏省公安厅	202.119.249.17:8080	弱口令	已修复	材料化学工程国家重点实验室
江苏省公安厅	202.119.249.17:8080	文件上传	已修复	材料化学工程国家重点实验室
江苏省公安厅	202.119.248.31:8080	文件上传	已关闭	国有资产管理处
江苏省教育网信办	202.119.242.22	系统信息泄露	已修复	信息服务部
教育 SRC	202.119.249.26	后台账号密码泄露	已修复	实验室建设与管理处
教育 SRC	202.119.243.205:7001	weblogic 未授权访问	已修复	校长办公室

教育 SRC	202.119.249.231:2181	未授权访问	已修复	后勤保障处
教育 SRC	115.28.107.134:8015	SQL 注入	已关闭	化学与分子工程学院

表一：汇漏洞通报汇总表

漏洞通报来源：



(三)学校僵尸主机发现

本月通过扫描发现校内学院机房存在部分僵尸主机，被植入恶意病毒，对校内其他设备发起攻击，给学校服务器和数据中心的正常运行带来了安全隐患。僵尸主机具体情况如下：

IP 地址	部门
10.13.119.72	计算机科学与技术学院
10.13.114.253	机械与动力工程学院

表二：僵尸主机汇总表

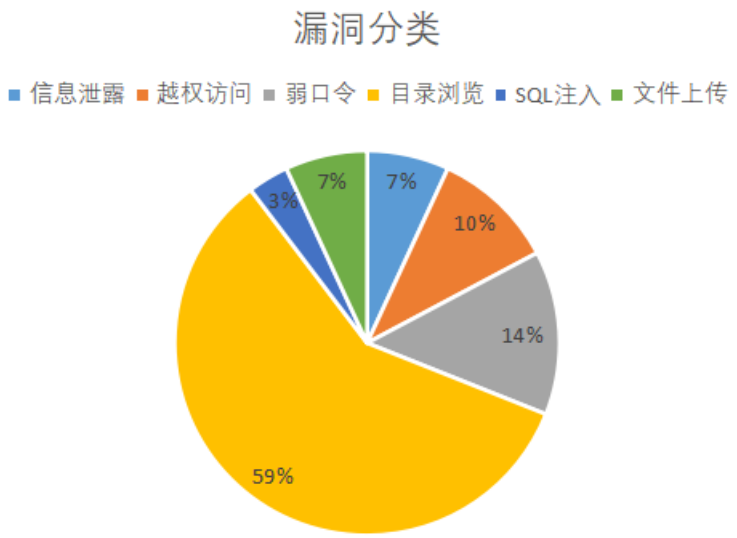
注：僵尸主机是指感染僵尸程序病毒，从而被黑客程序控制的计算机设备。该计算机设备可以是终端设备，也可以是云端设备。其可

以随时按照黑客的命令与控制（C&C，command and control）指令展开拒绝服务（DoS）攻击或发送垃圾信息。通常，一部被侵占的电脑只是僵尸网络里面众多中的一个，会被用来去运行一连串的或远端控制的恶意程序。一般电脑的拥有者都没有察觉到自己的系统已经被“僵尸化”，就仿佛是没有自主意识的僵尸一般。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 30 个。其中服务器弱口令 1 个，MongoDB 数据库弱口令 1 个，敏感信息泄露 3 个，越权访问 3 个，SQL 注入 1 个，文件上传 2 个，web 口令泄露 2 个，目录浏览 17 个。漏洞分类占比如下图：

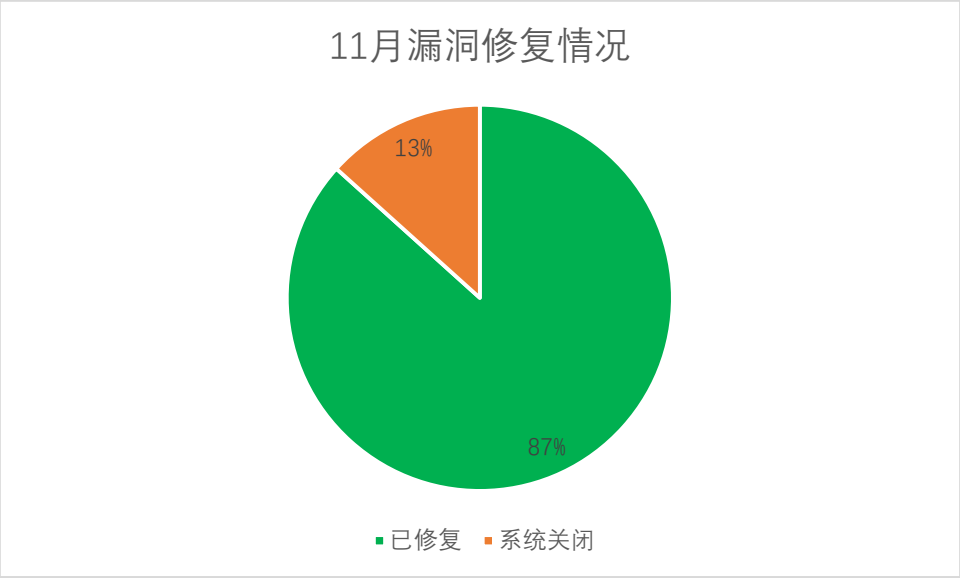


(二)漏洞修复情况

2020 年 11 月共发现漏洞 30 个。其中按时修复漏洞的有 26 个，因为漏洞无法修复，通过关停系统服务避免漏洞造成次生危害的漏洞有 4 个（见表三）。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
202.119.243.69:8500	高危	越权访问	实验室管理平台	实验室建设与管理处
202.119.249.68	高危	MongoDB 未授权	重点实验室环控	材料化学工程国家重点实验室
115.28.107.134:8015	中危	SQL 注入	虚拟仿真课程	化学与分子工程学院
202.119.248.31	高危	越权访问	招投标管理系统管理后台	国有资产管理处

表三：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
“双非”系统，网站未经登记直接在校外公有云上调试和发布	各部门需主动登记校外“双非”资产，签署“双非”系统安全责任状。通知各部门新系统上线前统一到信息中心登记管理，重要系统上线前要做安全渗透检测。
web 后台仍存在弱口令	系统管理员定期修改软件系统密码，密码必须为强密码。
网站测试文件未删除	新上线系统统一删除测试文件
部分网站后台管理多个网站	一个网站后台管理一个系统
网站未迁移到站群，缺少专人管理	网站迁移至网站群，将不需对校外提供服务的系统关闭对外访问权限，划分系统管理人，无对应管理人员的系统进行关闭处理。

四、网信安全每月小结

本月我校信息系统漏洞数量比上月有所提高，因各部门响应处理及时，未造成网络安全事件，但我校网络安全形势仍非常严峻，各单位需加强管理好服务器口令并满足密码策略要求，及时修补各种漏洞，定期关注服务器运行情况，以免被不法分子利用，对全校网络信息安全造成威胁。

网络与信息系统安全联系电话：58139275,83172363。

信息服务部

2020 年 12 月 4 日