2021 年网络与信息系统安全月报

（5 月）

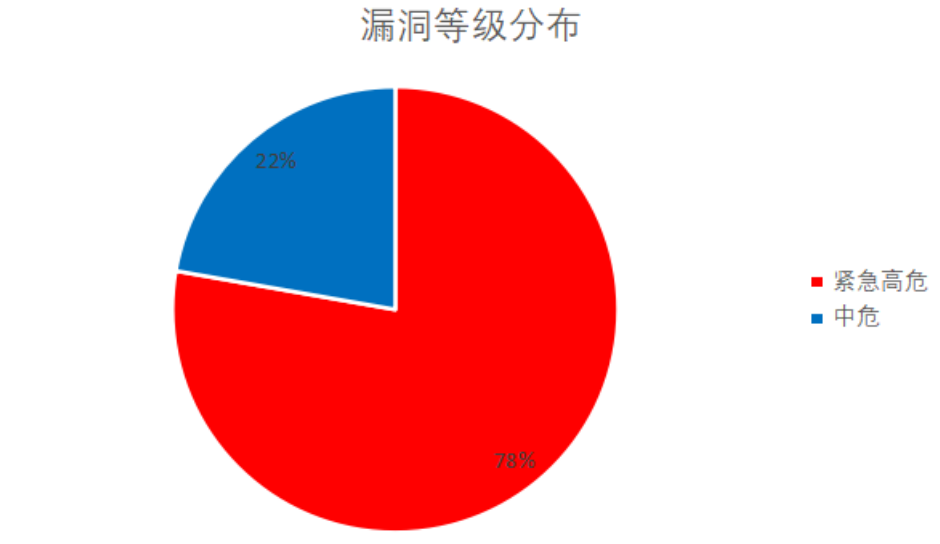
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 5 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 9 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 7 个，校外通报漏洞 2 个。其中紧急高危 7 个，中危漏洞 2 个，低危漏洞 0 个，紧急高危占比：77.7%。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，未造成重大网络安全事件。

漏洞通报的来源包括：江苏省委网信办，教育 SRC。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	http://emas.njtech.edu.cn	Shiro 命令执行	已修复	教务处
教育 SRC	202.119.250.123:27017	信息泄露	已修复	保卫处

表一：第三方通报漏洞

(三)非法外链情况

本月仍有多个系统及网站存在非法外链，具体情况如下：

网站（系统）	部门
http://jjxy.njtech.edu.cn	继续教育处
http://jgy.njtech.edu.cn/	经济与管理学院

表二：非法外链汇总表

(四)未进行安全检测违规上线情况

在江苏省委网信办组织的“2021年江苏省网络安全事件应急演练”中发现，我校教务处的试卷管理系统存在Apache Shiro反序列化远程代码执行漏洞，进而被获取主机权限，该漏洞极易演变为严重的网络安全事件。该试卷管理系统存在严重漏洞，并在未进行完整规范的安全渗透检测的前提下，擅自上线试运行，存在巨大安全风险。

（五）网安协查

2021年5月18日上午10点13分左右，我校接到上级公安机关的协查通知。协查通知中涉及我校两个系统：电气工程与控制科学学院的虚拟仿真课程，域名为http://virtual-a.eecs.njtech.edu.cn，对应IP地址为210.28.203.92；材料化学工程国家重点实验室的视频监控系统，对应IP地址是202.119.249.91。通过警方提供的材料及日志分析，我校视频监控系统服务器（202.119.249.91）和虚拟仿真课程服务器（210.28.203.92）被动成为对境外政府机关进行DDOS攻击的中转站。

通过调查和技术分析发现该两个系统都存在以下共性问题：

1.两个软件系统所在的服务器遭受了来自外界网络的大量攻击和扫描，未被攻陷。

2.两台软件系统的服务器都安装了FTP服务软件，对外提供ftp文件上传下载服务。操作系统没有攻陷的前提下，网络攻击者利用ftp协议的漏洞和ftp服务软件的漏洞，把两台服务器变成数据中转站，对境外政府机关网站进行攻击。

针对以上情况，学校及时做出了以下处理措施：在边界防火墙关闭210.28.203.92和202.119.249.91的21端口。同时对校园网IP端

口服务统一要求：原则上不再对外放开 21,22,3389 等远程管理端口，web 服务默认开放 80 和 443 端口，信息系统做过安全渗透测试后方可正式上线对互联网提供服务。

（六）校内攻防演练

2021 年 5 月 24 日，我校对校内信息系统（网站）进行网络安全攻防演练，成功获得后勤保障处洗浴热水运行监控平台（202.119.249.108）、教务处智慧教室互动教学平台（202.119.249.129）两个系统控制权，两个系统都存在弱口令漏洞。获得化学与分子工程学院实验教学智能管理系统（202.119.249.57）控制权，该系统存在的 SQL 注入和文件上传漏洞，并对该系统主页进行了篡改。

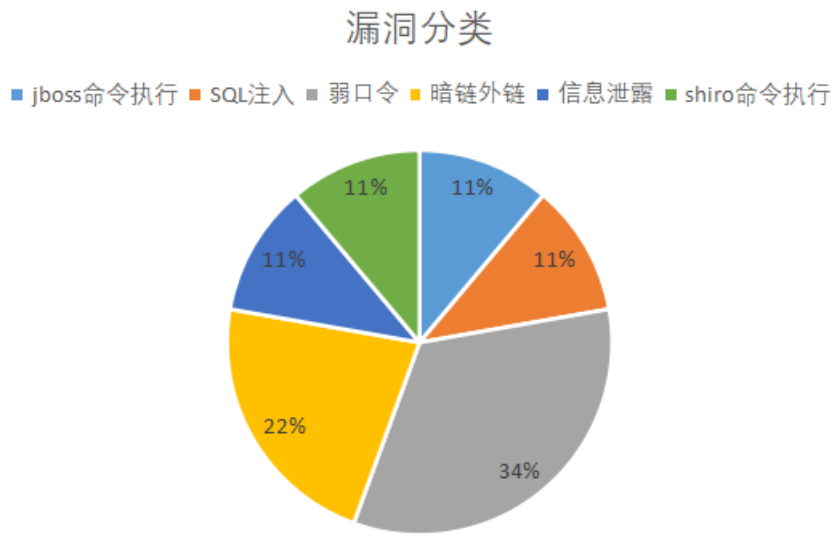
演练攻陷后，信息管理中心根据《南京工业大学校园网络与信息安全应急处置预案》进行了及时处置，并通知相关单位负责人对漏洞进行修复。

通过本次演练，发现部分业务单位对网络安全工作重视程度仍然不够，对网络安全事件紧急处理反应迟缓。后期学校会不定期进行网络应急攻防演练，以练促防，提高各单位应急响应能力。

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 9 个。其中暗链外链 2 个，弱口令 3 个，SQL 注入 1 个，jboss 命令执行 1 起，shiro 命令执行 1 起，信息泄露 1 个。漏洞分类占比如下图：



注：

Jboss 是 web 服务器的一种，是用来提供 web 服务的一款软件。Jboss 命令执行是指利用该款软件的漏洞进行远程攻击形式。软件供应商必须正确配置 Jboss 软件，并及时对该软件进行升级打补丁，才能减少此类漏洞的出现。

Shiro 命令执行是指利用 Apache Shiro（一种功能强大且易于使用的 Java 安全框架，它具有身份验证、访问授权、数据加密、会话管理等功能，可用于保护任何应用程序的安全）的漏洞，进行远程攻击的形式。软件供应商必须正确配置 Apache Shiro，并及时对该软件进行升级打补丁，才能减少此类漏洞的出现。

(二)漏洞修复情况

2021 年 5 月共发现漏洞 9 个，本月漏洞均已修复。

三、安全威胁风险与防范

（一）传统安全威胁风险与防范

安全威胁风险	防范措施建议
暗链外链情况较多	加强扫描力度，定期清除过期的新闻公告。
弱口令存在较多	加大运维管理员口令安全意识，定期检查系统密码复杂度。
系统安全管理风险	信息系统（网站）在正式上线运行前，需要完成安全检测。运行期间要及时打安全补丁，修补漏洞。

软件发布时候使用的 web 服务软件，软件中调用的通用功能模块的漏洞存在漏洞，造成软件易被攻击	及时、主动更新 web 服务软件，以及软件中调用的通用功能模块至最新版本。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，但本月暴露的安全问题不容乐观，个别信息系统未经安全渗透检测就上线试运行，存在巨大安全风险；部分信息系统对外开放端口没有做好安全防护，成为被攻击的入口。各单位应全面梳理本单位的信息资产，并做好安全防护工作，严格按照信息管理中心要求安装操作系统防护软件，新建信息系统未经过安全渗透检测，一律不得上线。同时要求各单位时刻绷紧安全之弦，高度认识网络安全和信息化工作的极端重要性，从讲政治的高度严格落实网络安全责任制。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 6 月 2 日