2021 年网络与信息系统安全月报

(1 月)

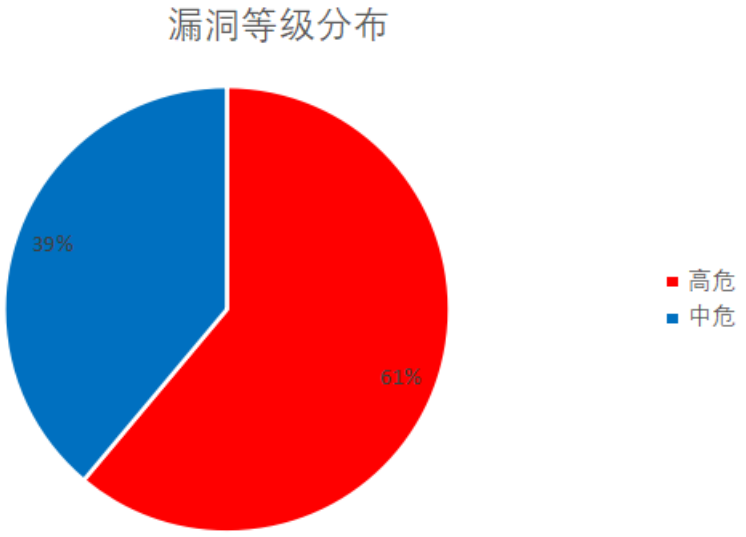
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 1 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 18 个。通过校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 17 个，校外通报漏洞 1 个。其中紧急高危 11 个，中危漏洞 7 个，低危漏洞 0 个，紧急高危占比：61%。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)第三方漏洞通报情况

我校 1 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：江苏省教育网信办。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
江苏省教育网信办	http://atc.mce.njtech.edu.cn/	备份文件下载	已修复	材料化学工程国家重点实验室

表一：第三方通报漏洞

(三)非法外链

本校 1 月份检查到多个系统及网站存在非法外链或存在非法信息，具体情况如下：

网站	部门
http://gra.njtech.edu.cn/	研究生院
http://2011.njtech.edu.cn/	国家“江苏先进生物与化学制造”协同创新中心
http://www.geonjut.com/（“双非”系统）	交通运输工程学院
http://trans.njtech.edu.cn/	交通运输工程学院
https://safety.njtech.edu.cn/	实验室建设与管理处

表二：非法外链汇总表

（四）“双非”系统未登记备案

本校 1 月份检查到交通运输工程学院岩土工程研究所网站（http://www.geonjut.com/），架设在校外并存在非法链接被通管局通报。该网站属于“双非”信息资产，未及时登记备案，也未签署“双非”系统安全责任状，目前该网站已关停。

（五）僵尸病毒

本月通过检测，发现本校一台服务器被黑客植入僵尸病毒，攻击者通过该病毒进行权限控制、威胁扩散、信息窃取以及信息破坏等高危操作。

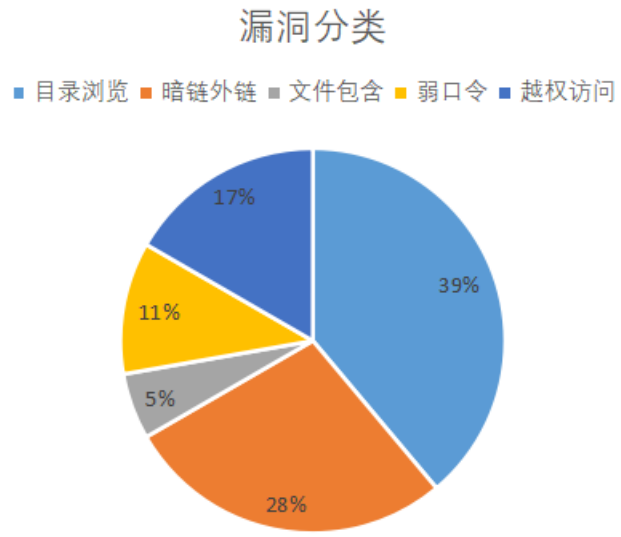
IP 地址	部门
10.13.114.254	机械与动力工程学院

表三：感染僵尸病毒主机汇总表

二、安全情况分析

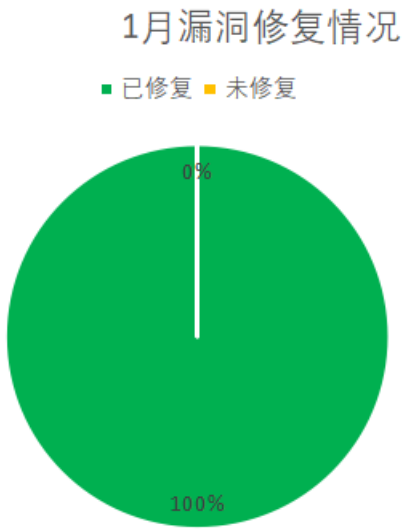
(一)漏洞类型分析

本月共发现漏洞 18 个，其中目录浏览 7 个，暗链外链 5 个，文件包含 1 个，弱口令 2 个，越权访问 3 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 1 月共发现漏洞 18 个，其中按时修复漏洞的有 18 个。具体情况如下：



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
WEB 登录存在弱口令	加强口令管理意识，删除测试使用的账号密码。
非法外链情况较多	定期清除过期的新闻公告，在新闻公告中尽

	量不写网址链接。详见南工校信〔2020〕3号《关于加强我校网站中外部链接管理的通知》
“双非”系统，网站未经登记直接在校外服务器上调试和发布	各部门需主动登记“双非”信息资产，签署“双非”系统安全责任状。各部门新系统上线前需统一到信息管理中心登记管理，重要系统上线前要做安全渗透检测。

注：“双非”信息资产定义：

1.使用校外 IP，但采用 njtech.edu.cn 学校域名后缀；

2.使用校内 IP，但采用非 njtech.edu.cn 后缀；

3.使用校外 IP、非 njtech.edu.cn 后缀，但内容与南京工业大学相关。

（二）僵尸病毒威胁风险与防范

僵尸网络病毒，通过连接 IRC 服务器进行通信从而控制被攻陷的计算机。僵尸网络(英文名称叫 BotNet)，是互联网上受到黑客集中控制的一群计算机，往往被黑客用来发起大规模的网络攻击，如分布式拒绝服务攻击(DDoS)、海量垃圾邮件等，同时黑客控制的这些计算机所保存的信息也都可被黑客随意“取用”。

案例：2017 年 10 月，一个名为“IoT_reaper”的新型僵尸网络出现。该僵尸网络利用路由器、摄像头等设备的漏洞，将僵尸程序传播到互联网，感染并控制大批在线主机，从而形成具有规模的僵尸网络。目前，很多厂商的公开漏洞都已经被 IoT_reaper 病毒所利用，其中包括 Dlink(路由器)、Netgear(路由器)、Linksys(路由器)、Goahead（摄像头）、JAWS（摄像头）、AVTECH（摄像头）、Vacron（NVR）等共 9 个漏洞，感染量达到近 200 万台设备，且每天新增感染量达 2300 多次。

防护手段：关闭不必要端口，卸载不必要的程序，定期进行安全检查和加固。启用入侵检测防护设备用于发现异常情况并进行告警和阻断，使用下一代防火墙进行防护，将资产放入 WEB 应用防火墙。

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，因各部门响应处理及时，未造成网络安全事件，但还存在“双非”信息资产没有登记报备的情况，请各单位各部门高度重视，主动登记“双非”信息资产。各二级网站系统中非法外链问题也不容乐观，需网站系统负责人与信息发布者及时关注，定期清除所属网站失效链接以及过期新闻公告。网信安全问题需要师生长期关注，时刻保持警惕，共同维护我校网络与信息系统安全。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 2 月 1 日