2021 年网络与信息系统安全月报

（7 月）

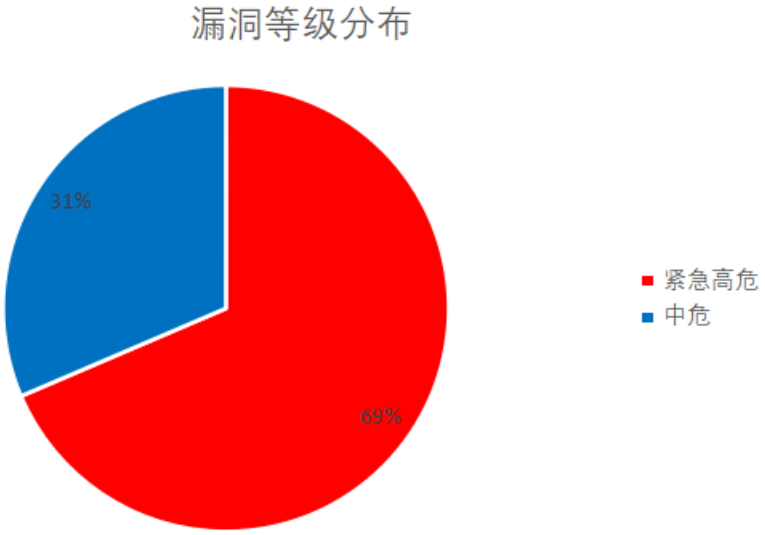
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 7 月份网络与信息系统安全情况通报如下：

一、本月整体安全情况

(一) 漏洞发现情况

本月共发现漏洞 35 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 33 个，校外通报漏洞 2 个。其中紧急高危 24 个，中危漏洞 11 个，低危漏洞 0 个，紧急高危占比：69%。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，未造成网络安全事件。

漏洞通报的来源包括：教育 SRC，南京市公安局。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 SRC	https://jwgl.njtech.edu.cn/	信息泄露	已修复	教务处
南京市公安局	http://myoa.njtech.edu.cn	Weblogic 命令执行	已修复	校长办公室

表一：第三方通报漏洞

(三)非法外链情况

本月检查到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://hgy.njtech.edu.cn/	化工学院
http://cise.njtech.edu.cn/	计算机科学与技术学院
http://spy.njtech.edu.cn/	食品与轻工学院
http://trans.njtech.edu.cn/	交通运输工程学院

http://eecs.njtech.edu.cn/	电气工程与控制科学学院
http://tyxy.njtech.edu.cn/	体育学院
http://cces.njtech.edu.cn/	安全科学与工程学院
http://spy.njtech.edu.cn/	食品与轻工学院
http://kyy.njtech.edu.cn/	科学研究院
http://jgy.njtech.edu.cn/	经济与管理学院

表二：非法外链汇总表

(四)挖矿病毒

本月对本校服务器和终端做了挖矿病毒专项检查，检查中发现多个机房的终端存在大规模感染挖矿病毒情况，具体情况如下：

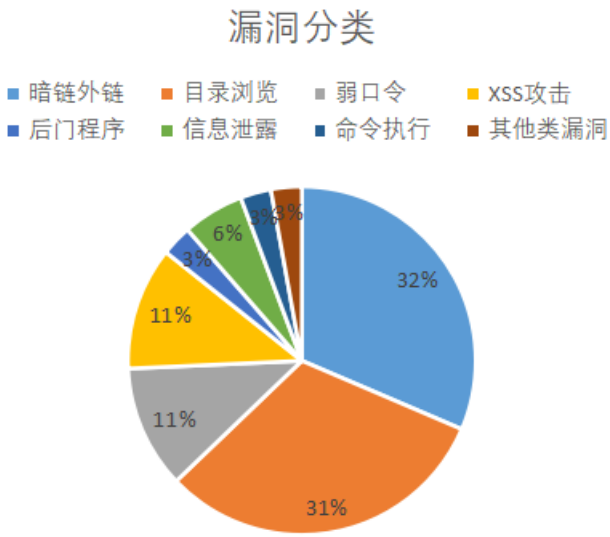
IP 地址	部门
10.3.129.*	经济与管理学院
10.3.131.*	经济与管理学院
10.3.132.*	经济与管理学院

表三：感染病毒主机汇总表

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 35 个。其中暗链外链 11 个，目录浏览 11 个，XSS 攻击 4 个，弱口令 4 个，后门程序 1 个，信息泄露 2 个，命令执行 1 个，其他类漏洞 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2021 年 7 月共发现漏洞 35 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
弱口令数量较多	加大运维管理员口令安全意识，定期检查系统密码复杂度。
不安全端口存在高危漏洞	加强运维管理，不必要对外开放的端口限制在本地访问。
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。

（二）挖矿病毒威胁风险与防范

互联网的虚拟货币，如比特币（BTC）、门罗币（XMR）等，一种由开源的 P2P 软体产生的网络电子虚拟货币。虚拟货币挖矿是一种复杂的机器运算行为。通常，进行挖矿的矿

工需要大规模、高功效的计算设备，进行长时间的运算，从而获取虚拟货币，牟取利益。

感染风险说明：

1、主机长时间执行高性能计算，浪费网络带宽，CPU 和内存占用较高，不能及时处理用户的正常请求或任务。

2、增加电力消耗，加快 CPU、内存等硬件老化速度。

3、同时挖矿软件已经被植入受害主机，表明主机很可能已被黑客控制，现有的安全防护体系已经部分甚至完全失效，还存在以下潜在风险：

（1）黑客通过挖矿程序窃取机密信息，比如机密文件、关键资产的用户名和密码等，导致企事业单位遭受更进一步的资产损失。

（2）黑客控制主机作为“肉鸡”攻击互联网上的其他单位，违反网络安全法，遭致网信办、网安等监管单位的通报处罚。

（3）黑客利用已经控制的机器，作为继续对内网渗透的跳板，产生更严重的网络安全攻击事件。

处置与防范建议：

1、关注服务器及终端是否对外发生恶意连接行为，挖矿病毒会对矿池进行恶意连接。

2、服务器及终端安装杀毒软件，启用防火墙功能。

四、网信安全每月小结

本月我校信息系统漏洞总数量较多，各部门响应处理及时，未造成网络安全事件。但是网站暗链外链，敏感信息泄露，弱口令等漏洞仍然层出不穷，说明部分信息系统及网站仍存在较大安全隐患。各部门应严格遵守学校网络安全各项工作要求，始终保持警惕，克服麻痹思想，确保信息系统安全。

网络与信息系统安全联系电话：58139275,83172363。

信息管理中心

2021 年 7 月 31 日