2023 年网络与信息系统安全月报
（6 月）

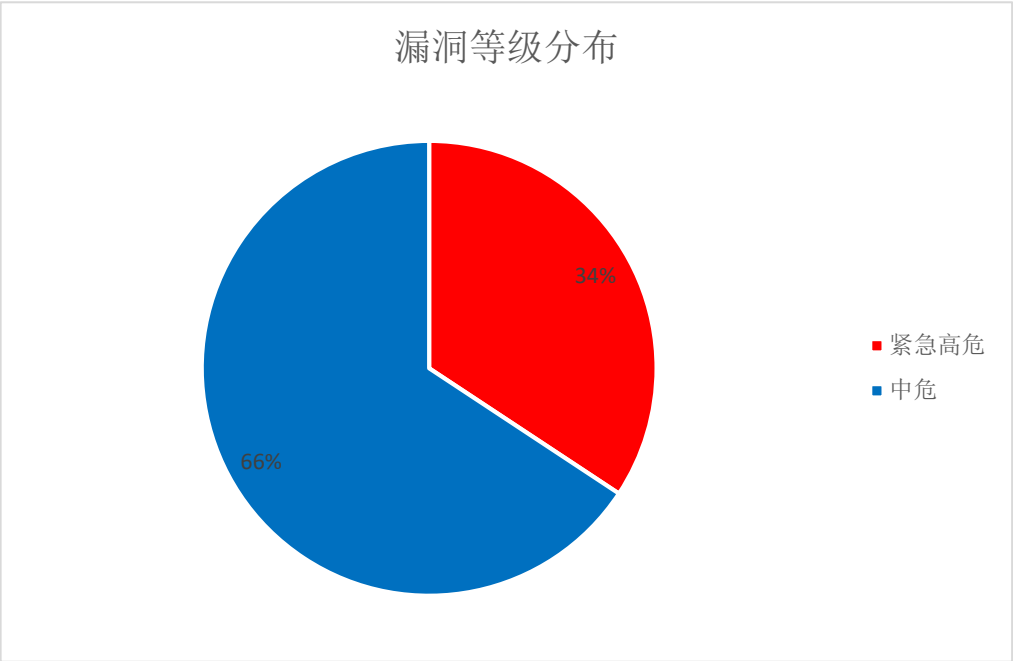
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将6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 23 个，校外通报漏洞 4 个，外链 8 个。其中紧急高危 12 个，中危漏洞 22 个，低危漏洞 0 个，紧急高危占比：35%。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

本月第三方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。

通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 src	rlcj.njtech.edu.cn	信息泄露	已修复	保卫处
教育 src	rlcj.njtech.edu.cn	任意文件上传	已修复	保卫处
教育 src	xsgl.njtech.edu.cn	弱口令	已修复	学生工作处
教育 src	psy.yunxinli.cn（双非系统）	弱口令	已修复	学生工作处

（三）非法外链情况

本月检查到 3 家单位所属网站共出现 8 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://jjc.njtech.edu.cn/	基本建设处	6 次	通信管理局
https://alumni.njtech.edu.cn	对外合作与发展处	1 次	通信管理局
https://chem.njtech.edu.cn	化学与分子工程学院	1 次	通信管理局

（四）网络安全攻防演练

根据省网信办“网安 2023”文件精神，6 月 13 日，信息管理中心根据学校信息化年度工作安排进行网络安全攻防演练。此次演练针对我校信息系统出现较多的弱口令、SQL 注入以及后台越权等漏洞展开，演练对象为：测绘科学与技术学院的虚拟仿真平台（http://virtual.njtech.edu.cn），化学与分子工程学院的虚拟仿真教学平台（http://202.119.249.57:8090），大学科技园管理办公室的微信小程序后端平台（http://202.119.248.130），三个系统均被攻陷。

实战安全演练过程中化学与分子工程学院及时响应，在演练后的半小时内及时响应并应急处理并修复了漏洞，其余参加演练的两个部门未能及时响应，由信息管理中心对该系统进行断网处理，并通过校网信通报平台通知到相关部门的负责人。

此次演练聚焦学校重点网站、重要信息系统的实体安全、运行安全和数据安全，模拟在面对网络安全突发事件时，如何妥善应对处置，最大限度地减少事件产生的危害，维护学校网络安全。

在演练过程中，暴露了部分二级单位（部门）对网络安全的重视度不足，应急处理能力不足的情况。

（五）处置“挖矿病毒”

6月15日，信息管理中心监测发现我校部分学院自用计算服务器感染了挖矿病毒，导致服务器无法正常运行，通过技术手段，发现感染来源是计算机学院某老师名下的一台电脑（IP 地址：10.3.89.*，MAC 地址：5811.22c5.22**）。

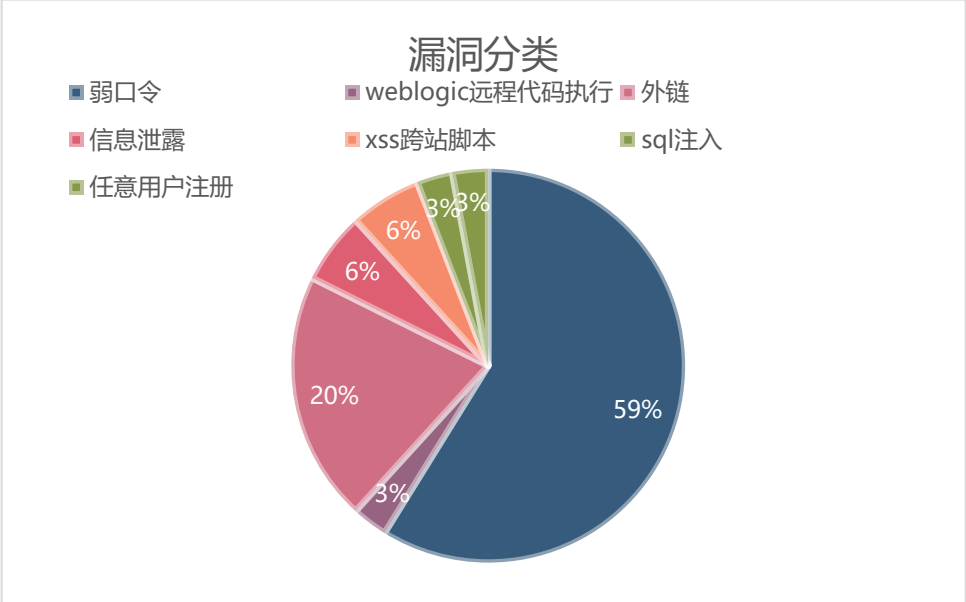
经过调查该电脑由于设置了弱口令，并长期处于网络在线状态，且未安装杀毒软件，导致电脑被非法入侵，成为挖矿病毒攻击的来源。被挖矿病毒感染的计算用服务器中招的主要原因也是由于服务器存在弱口令问题，服务器没有设置任何防护策略导致的。

请各单位高度重视单位内部自行架设并使用的计算服务器存在的大量弱口令问题。

二、本月整体安全情况

（一）漏洞类型统计

本月共发现漏洞35个。其中暗链外链8个，弱口令20个，SQL注入1个，weblogic远程命令执行1个，任意用户注册1个，信息泄露2个、xss跨站脚本2个。漏洞分类占比如下图：



（二）漏洞修复统计

本月共发现漏洞 35 个，均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
网站弱口令较多	加强人员网络安全防范意识，定期修改网站登录密码。
网页存在暗链外链	定期排查网页外链，清除过期链接，避免被恶意抢注为非法网站。
网站配置文件泄露	服务器禁止备份网站文件，禁止将配置文件泄露到公网，加强网站访问目录权限限制。

四、网信安全每月小结

本月我校信息系统漏洞总数量较多，因各部门响应处理及时，

未造成网络安全事件。本月安全漏洞情况较多，暗链外链和弱口令情况比较严重，各单位需定期修改口令，删除过期链接和新闻，加强网络安全防范意识，以更强烈的担当、更主动的作为、更严实的作风、更有力的措施，把学校的网络安全保障工作抓紧做实，齐心协力共同筑牢网络安全工作防线。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023 年 7 月 7 日