2022年网络与信息系统安全月报

（10月）

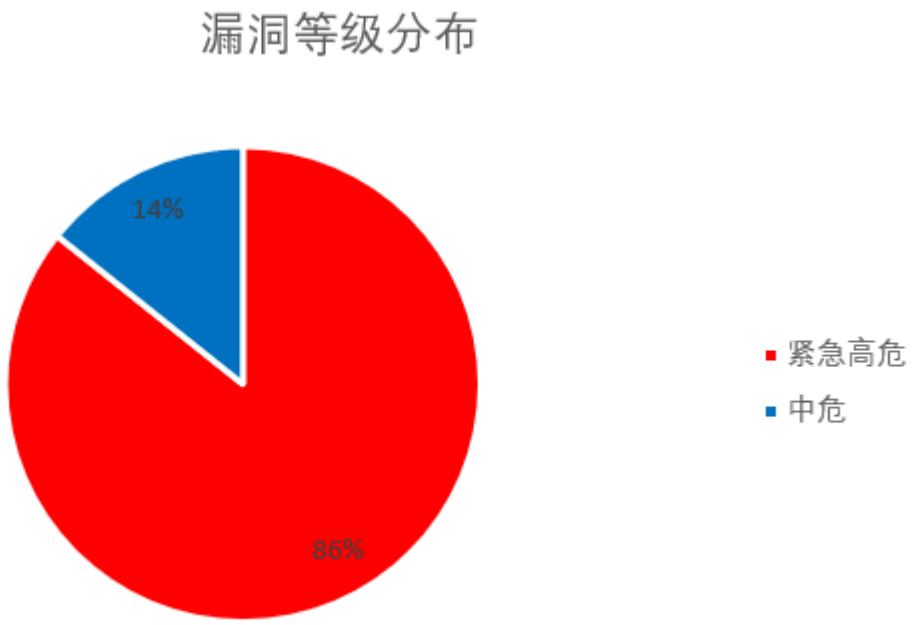
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将10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

本月共发现漏洞7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，校外通报漏洞0个。其中紧急高危6个,中危漏洞1个,低危漏洞0个,紧急高危占比:86%。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

本月未收到第三方漏洞通报。

(三)非法外链情况

本月检查到 1 家单位所属网站共出现 1 次非法外链,具体情况如下:

网站（系统）	部门	频次
http://tyxy.njtech.edu.cn/	体育学院	1 次

(四)挖矿病毒处置

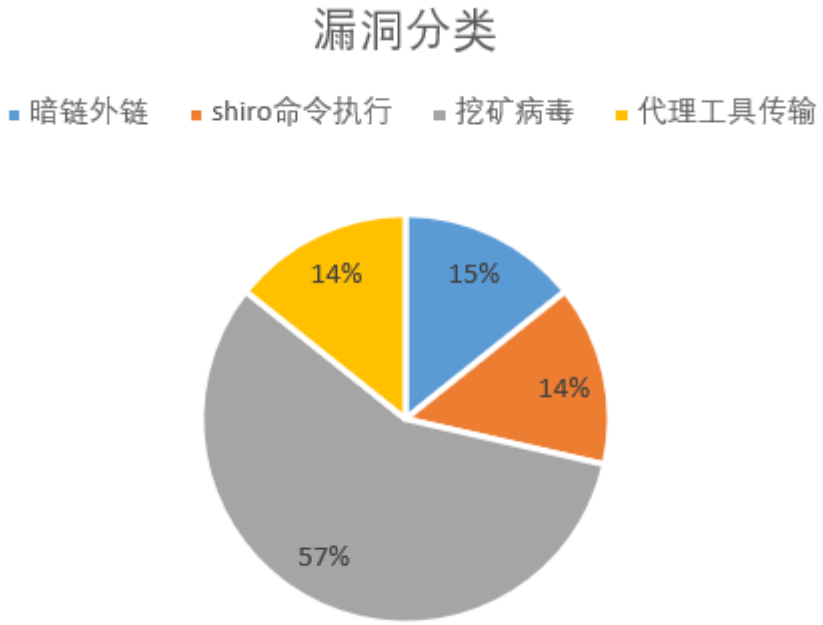
本月信息管理中心监测发现校内多台服务器或终端感染挖矿病毒，感染服务器或者终端通过远程下载可执行脚本进行挖矿并攻击其他段服务器和终端，信息管理中心立刻组织网络安全专业人员处理，确定了攻击来源和攻击手段，对感染服务器和终端进行了网络隔绝，阻断了感染途径。信息管理中心指导涉事服务器和终端所属人员进行全面杀毒和重装系统，未对校内正常科研和学习生活造成进一步影响。

感染病毒设备网段	矿池地址	所属单位
10.10.132.*	141.164.47.246	柔性电子（未来技术）学院
10.249.249.*	206.190.238.3	计算机科学与计算学院
10.3.11.*	199.247.27.41	教务处
202.119.249.*	182.92.208.116	智能制造研究院

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 7 个。其中暗链外链 1 个， shiro 命令执行 1 个，挖矿病毒 4 个，代理工具传输 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2022 年 10 月共发现漏洞 7 个，本月漏洞均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
我校挖矿病毒较多	加强网络安全监测，服务器和终端需安装病毒防护软件。
系统版本存在高危漏洞	定期针对系统做漏洞扫描，安装软件版本确认无问题在安装。

四、网信安全每月小结

本月各单位在重点保障时期加强网络安全工作组织部署，积极开展网络安全隐患排查和整改，切实做好安全监测预警通报工作，建立网络安全应急响应机制，加强值班值守和信息报送，确保全校网络与信息系统持续安全稳定，顺利完成了二十大期间的网络安全保障工作。

网络与信息系统安全联系电话：58139275。

信息管理中心

2022 年 11 月 17 日