# 中国地质大学（武汉）网络安全月报

2023 年 4 月　（第 W0085 期）　总第 85 期

中国地质大学（武汉）信息化工作办公室　2023 年 4 月 30 日

## 1、情况综述

根据监测分析，4 月份我校校园网络发生的安全威胁事件共计 594180 起。其中服务器受到攻击的事件 593977 起、蠕虫病毒攻击事件 11 起、木马病毒攻击事件 192 起、来自外部的 DoS 攻击事件 0 起。

4 月份我校总体网络安全情况良好，处理网络安全事件共 7 起，未发生重大的网络安全事件,后续会继续保持和完善。

## 2、安全事件通报

4 月处理网络安全事件共 7 起。其中，学校内部自查 5 起，教育部漏洞报告平台通报 1 起，教育系统网络安全工作管理平台安全监测预警子系统通报 1 起。

**网络安全事件汇总表**

| 序号 | 时间 | 内容 | 处理结果 |
|---|---|---|---|
| 1 | 4 月 6 日 | 学校内部自查发现某信息系统存在敏感信息泄露问题 | 已整改 |
| 2 | 4 月 6 日 | 学校内部自查发现某信息系统存在敏感信息泄露问题 | 已整改 |
| 3 | 4 月 8 日 | 学校内部自查发现某信息系统存在暗链问题 | 已整改 |
| 4 | 4 月 8 日 | 学校内部自查发现某信息系统存在暗链问题 | 已整改 |
| 5 | 4 月 21 日 | 教育部漏洞报告平台通报某信息系统存在弱口令、系统设计问题 | 已整改 |
| 6 | 4 月 24 日 | 学校内部自查发现某信息系统存在敏感信息泄露问题 | 已整改 |
| 7 | 4 月 27 日 | 教育系统网络安全工作管理平台安全监测预警子系统通报某信息系统存在暗链问题 | 已整改 |

## 3、服务器受攻击情况

本次监测时间为 4 月，防火墙防护服务器受到攻击事件共 593977 起；其中针对学校门户站群系统的攻击次数达到 83864 起，占总数的 14.12%。门户站群系统提供我校 213 个各类的管理、发布功能，通过入侵防御、病毒木马防护及 Web 应用防护等手段，可以有效防护攻击，保障安全。

**受攻击次数排名前五的服务器列表**

| 序号 | 目标服务器 IP/名称 | 攻击次数 |
|---|---|---|
| 1 | 站群系统 | 83864 |
| 2 | 校园虚拟专用（VPN）网络 | 11816 |
| 3 | 珠宝检测中心 | 7495 |
| 4 | 逸夫博物馆三维可视化系统 | 4937 |
| 5 | 图书馆主页 | 3672 |

## 4、信息系统漏洞扫描分析

本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现中高危漏洞 1029 个，其中高危漏洞 474 个，中危漏洞 555 个，漏洞数量较上月减少。

**存在中高危漏洞数量排名前十的信息系统**

| 序号 | 信息系统名称 | 中高危漏洞情况 |
|---|---|---|
| 1 | 高性能计算公共服务平台 | 高危漏洞 98 个，中危漏洞 127 个。 |
| 2 | 测试服务 | 高危漏洞 52 个，中危漏洞 38 个。 |
| 3 | 商业门面从业人员管理系统 | 高危漏洞 32 个，中危漏洞 24 个。 |
| 4 | 海洋学院导师制管理系统 | 高危漏洞 25 个，中危漏洞 14 个。 |
| 5 | 中国地质大学（武汉）人才信息系统 | 高危漏洞 24 个，中危漏洞 15 个。 |
| 6 | 国际会议申报系统 | 高危漏洞 21 个，中危漏洞 16 个。 |
| 7 | 实验室安全巡检平台 | 高危漏洞 15 个，中危漏洞 9 个。 |
| 8 | 数据共享 web 网站 | 高危漏洞 14 个，中危漏洞 6 个。 |
| 9 | 基建项目管理系统（BS） | 高危漏洞 13 个，中危漏洞 12 个。 |
| 10 | 一卡通平台_运维监控平台 | 高危漏洞 11 个，中危漏洞 89 个。 |

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

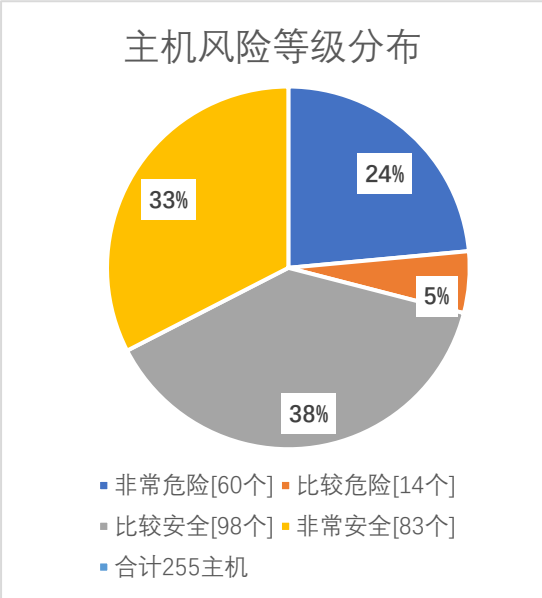
本月完成主机高危漏洞整改 32 个、主机中危漏洞整改 70 个。

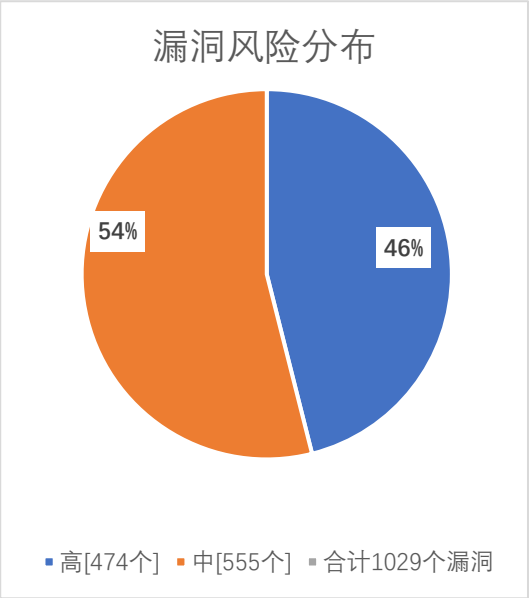
因新漏洞库更新，本月新增网站高危漏洞 44 个，网站中危漏洞 27 个。

本月漏洞数量较上月减少，5 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

| 漏洞数量 | 高危漏洞 | 中危漏洞 | 合计 |
|---|---|---|---|
| 4 月 | 474 | 555 | 1029 |
| 3 月 | 462 | 598 | 1060 |
| 变化量（个） | 增多 12 个 | 减少 43 个 | 减少 31 个 |

在本月扫描的 255 台服务器中，主机、网站中高危漏洞总计 1029 个，其中高危漏洞 474 个，中危漏洞 555 个。主机风险等级中，非常危险的占 24%，比较危险的占 5%，比较安全的占 38%，非常安全的占 33%。漏洞风险等级中，高危漏洞占比 46%，中危漏洞占比 54%。




**影响主机数排名前十的漏洞种类**

| 危险程度 | 漏洞名称 | 影响主机数 |
|---|---|---|
| 高 | Nginx 安全漏洞（CVE-2022-3638） | 43 |
| 高 | Apache Tomcat 环境问题漏洞(CVE-2022-42252) | 23 |

| | | |
|---|---|---|
| 高 | Apache Tomcat 代码问题漏洞(CVE-2022-29885) | 15 |
| 高 | Eclipse Jetty 缓冲区错误漏洞(CVE-2009-5047) | 12 |
| 高 | Eclipse Jetty Dump Servlet 信息泄露漏洞(CVE-2009-5045) | 12 |
| 高 | Eclipse Jetty 安全漏洞(CVE-2020-27216) | 12 |
| 高 | SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】 | 11 |
| 高 | nginx 安全漏洞(CVE-2021-23017) | 10 |
| 高 | Apache Tomcat 权限许可和访问控制问题漏洞(CVE-2022-23181) | 6 |
| 高 | PHP 远程命令执行漏洞(CVE-2022-31626) | 5 |