

# 中国地质大学（武汉）网络安全月报

2023年10月（第W0091期）（发布） 总第91期

中国地质大学（武汉）信息化工作办公室

2023年10月31日

## 1、情况综述

根据监测分析,10月份我校校园网络发生的安全威胁事件共计4217107起。其中服务器受到攻击的事件4215578起、蠕虫病毒攻击事件1起、木马病毒攻击事件1528起、来自外部的DoS攻击事件0起。

10月份我校总体网络安全情况良好,处理网络安全事件共9起,未发生重大网络安全事件,后续会继续保持和完善。

## 2、安全事件通报

10月处理网络安全事件共9起。其中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6起,学校内部自查事件2起,教育部通报1起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	10月8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学校某信息系统存在暗链问题	已整改
2	10月8日	教育部通报某信息系统存在双非问题	已整改
3	10月10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学校某信息系统存在暗链问题	已整改
4	10月18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学校某信息系统存在暗链问题	已整改
5	10月18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学校某信息系统存在暗链问题	已整改
6	10月20日	学校内部自查发现某信息系统2存在SQL注入问题	已通报
7	10月20日	学校内部自查发现某信息系统存在XXE漏洞、系统敏感文件读取等严重问题	已通报

8	10月25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学校某信息系统存在暗链问题	已整改
9	10月31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学校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10月，防火墙防护服务器受到攻击事件共4215578起；其中针对学校门户网站群系统的攻击次数达到98600起，占总数的2.33%。门户网站群系统提供我校189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	校园虚拟专用（VPN）网络	349477
2	虚拟仿真平台	159074
3	地球科学在线	137622
4	远程教学学习管理系统	85048
5	“国际青年学者地大论坛”报名系统	71168

### 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：共发现中高危漏洞1301个，其中高危漏洞639个，中危漏洞662个，漏洞数量较上月少量增多。

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	存在高危漏洞128个，中危漏洞103个
2	测试服务	存在高危漏洞53个，中危漏洞37个
3	云因出版ERP管理系统	存在高危漏洞48个，中危漏洞73个
4	商业门面从业人员管理系统	存在高危漏洞48个，中危漏洞26个
5	海洋学院导师制管理系统	存在高危漏洞41个，中危漏洞16个
6	中国地质大学（武汉）人才信息系统	存在高危漏洞40个，中危漏洞17个
7	一卡通平台_运维监控平台	存在高危漏洞21个，中危漏洞136个
8	档案应用系统	存在高危漏洞20个，中危漏洞0个
9	远程教学管理平台2	存在高危漏洞18个，中危漏洞4个
10	网络报修系统	存在高危漏洞10个，中危漏洞10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

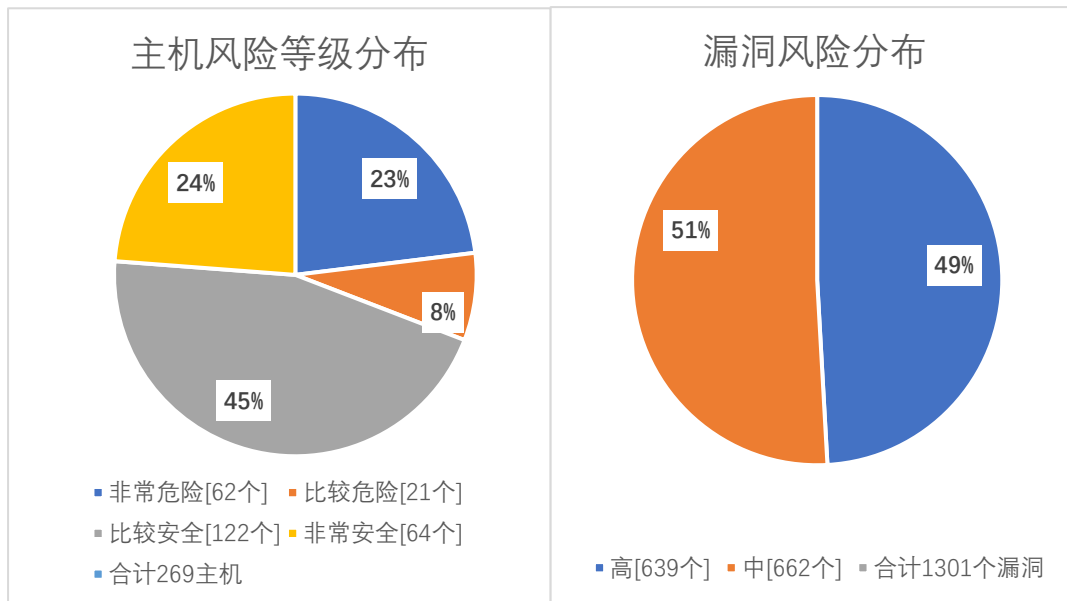
收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

本月完成 WEB 中危漏洞整改 20 个。因备案系统增多及漏洞库更新，本月新增主机高危漏洞 9 个，主机中危漏洞 2 个；WEB 高危漏洞新增 20 个。

本月漏洞数量较上月少量增多，11 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
10 月	639	662	1301
9 月	610	682	1292
变化量（个）	增加 29 个	减少 20 个	增加 9 个

在本月扫描的 269 台服务器中，主机、网站中高危漏洞总计 1301 个，其中高危漏洞 639 个，中危漏洞 662 个。主机风险等级中，非常危险的占 23%，比较危险的占 8%，比较安全的占 45%，非常安全的占 24%。漏洞风险等级中，高危漏洞占比 49%，中危漏洞占比 51%。



### 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	Apache Tomcat 拒绝服务漏洞 (CVE-2023-24998)	41

高	Apache Tomcat 注入漏洞(CVE-2022-45143)	38
高	nginx 缓冲区错误漏洞(CVE-2022-41741)	32
高	nginx 越界写入漏洞 (CVE-2022-41742)	32
高	Apache Tomcat 环境问题漏洞(CVE-2022-42252)	21
高	Eclipse Jetty 缓冲区错误漏洞(CVE-2009-5047)	15
高	Eclipse Jetty Dump Servlet 信息泄露漏洞(CVE-2009-5045)	15
高	Eclipse Jetty 安全漏洞(CVE-2020-27216)	15
高	Apache Tomcat 代码问题漏洞(CVE-2022-29885)	13
高	Apache Tomcat 安全漏洞(CVE-2023-28709)	7