中国地质大学（武汉）网络安全月报

2024 年 11 月　（第 W00104 期）（发布）　总第 104 期

中国地质大学（武汉）信息化工作办公室　2024 年 11 月 30 日

1、情况综述

根据监测分析，11 月份我校校园网络发生的安全威胁事件共计 4449765 起。其中服务器受到攻击的事件 4449126 起、蠕虫病毒攻击事件 154 条起、木马病毒攻击事件 485 起、来自外部的 DoS 攻击事件 0 起。

11 月份我校总体网络安全情况良好，处理网络安全事件共 15 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

11 月处理网络安全事件共 15 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事件 6 起，湖北省教育厅通报事件 2 起，内部自查事件 7 起。在通报的 15 起安全事件中，已整改 11 个，剩余 4 个暂未整改，涉及数学与物理学院、远程与继续教育学院、自动化学院、机械与电子信息学院 4 个单位。

网络安全事件汇总表

序号	时间	内容	处理结果
1	11 月 4 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我校某网站存在信息泄露问题	已整改
2	11 月 5 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我校某信息系统存在暗链问题	已整改
3	11 月 5 日	湖北省教育厅通报我校某信息系统存在文件上传、信息泄露、命令执行问题	已整改
4	11 月 5 日	湖北省教育厅通报我校某信息系统威胁报告存在弱口令问题	已整改
5	11 月 5 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我校某信息系统存在信息泄露问题	已整改
6	11 月 7 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我校某网站存在暗链问题	已整改
7	11 月 8 日	学校内部自查发现某网站存在暗链问题	已整改
8	11 月 11 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我校某网站存在暗链问题	已整改

9	11 月 12 日	学校内部自查某信息系统存在任意文件上传漏洞问题	未整改
10	11 月 14 日	学校内部自查发现某网站存在敏感信息泄露问题	未整改
11	11 月 14 日	学校内部自查发现某网站存在敏感信息泄露问题	已整改
12	11 月 14 日	学校内部自查发现某网站存在暗链问题	未整改
13	11 月 15 日	学校内部自查发现某网站存在暗链问题	已整改
14	11 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我校某信息系统存在 SQL 注入问题	已整改
15	11 月 28 日	学校内部自查发现某网站存在暗链问题	未整改

3、服务器受攻击情况

本次监测时间为 11 月，防火墙防护服务器受到攻击事件共 4449126 起；其中针对学校门户站群系统的攻击次数达到 61957 起，占总数的 1.29%。门户站群系统提供我校 191 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	所属单位	攻击次数
1	第一站群	信息化工作办公室	50002
2	堡垒机	信息化工作办公室	45882
3	新站群系统	信息化工作办公室	18110
4	校园虚拟专用网络（VPN）	信息化工作办公室	11955
5	饮食服务中心物流系统	后勤保障部	8230

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 442 个，其中高危漏洞 215 个，中危漏洞 227 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	归属单位	中高危漏洞情况
1	信息门户 2.0	信息化工作办公室	存在高危漏洞 89 个，中危漏洞 68 个。
2	云因出版 ERP 管理系统	出版社	存在高危漏洞 48 个，中危漏洞 73 个。
3	电子签章系统	信息化工作办公室	存在高危漏洞 9 个，中危漏洞 4 个。
4	学校办公平台	学校办公室	存在高危漏洞 8 个，中危漏洞 6 个。
5	融合出版平台	出版社	存在高危漏洞 8 个，中危漏洞 5 个。

6	远程教学大数据集群	远程与继续教育学院	存在高危漏洞 5 个，中危漏洞 6 个。
7	线下办事大厅综合管理平台	信息化工作办公室	存在高危漏洞 4 个，中危漏洞 2 个。
8	中国地质大学资产综合管理系统	财务与资产管理部	存在高危漏洞 4 个，中危漏洞 6 个。
9	智慧校园知识库平台	信息化工作办公室	存在高危漏洞 2 个，中危漏洞 0 个。
10	CARSI 登录服务器	信息化工作办公室	存在高危漏洞 2 个，中危漏洞 2 个。

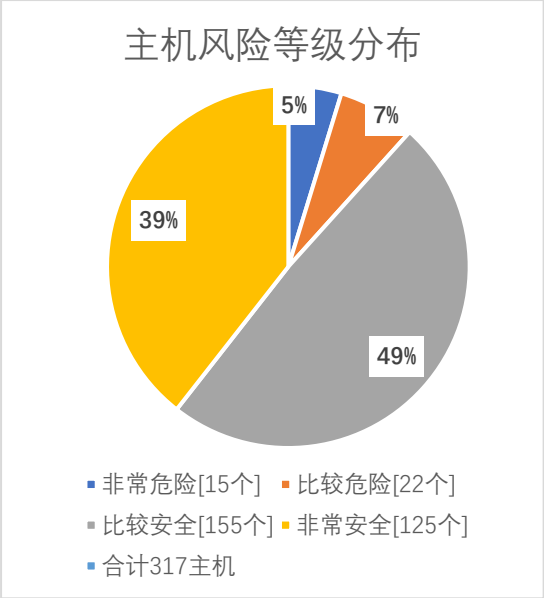
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

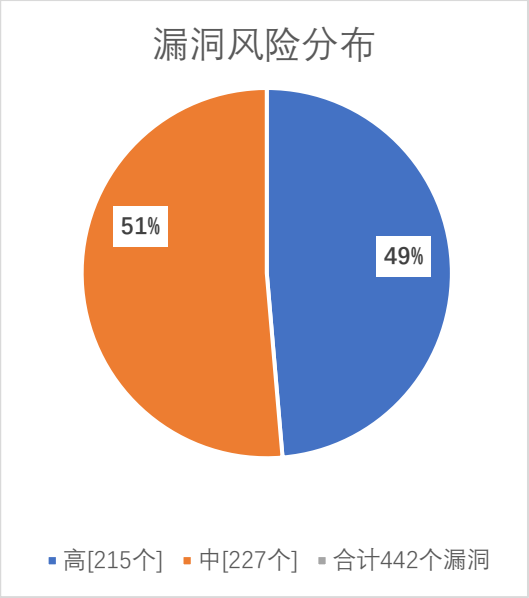
本月完成主机高危漏洞整改 47 个，主机中危漏洞整改 469。因新业务上线及漏洞库更新，本月新增主机高危漏洞 2 个，主机中危漏洞 2 个，WEB 高危漏洞 18 个。

本月漏洞数量较上月减少，12 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**
11 月	215	227	442
10 月	242	694	936
变化量（个）	减少 27 个	减少 467 个	减少 494 个

在本月扫描的 317 台服务器中，主机、网站中高危漏洞总计 442 个，其中高危漏洞 215 个，中危漏洞 227 个。主机风险等级中，非常危险的占 5%，比较危险的占 7%，比较安全的占 449%，非常安全的占 39%。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	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	4
高	Apache Tomcat CORS Filter 安全漏洞(CVE-2018-8014)	2
高	Apache Tomcat 远程代码执行漏洞(CVE-2017-12617)	2
高	Apache Tomcat 拒绝服务漏洞(CVE-2018-1336)	2
高	Apache Tomcat 安全限制绕过漏洞(CVE-2018-8034)	2
高	Apache Tomcat 安全漏洞(CVE-2021-25329)	2
高	检测到远端 X 服务正在运行中(CVE-1999-0526)	1
高	Oracle Database Server Java VM 组件安全漏洞(CVE-2018-3110)	1
高	Oracle Database Server OJVM 本地安全漏洞(CVE-2017-10202)	1
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	2