

中国地质大学（武汉）网络安全月报

2023年8月（第W0089期）（发布） 总第89期

中国地质大学（武汉）信息化工作办公室

2023年8月31日

1、情况综述

根据监测分析，8月份我校校园网络发生的安全威胁事件共计1670951起。其中服务器受到攻击的事件1669602起、蠕虫病毒攻击事件0起、木马病毒攻击事件1349起、来自外部的DoS攻击事件0起。

8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

8月处理网络安全事件共7起。其中教育部漏洞报告平台通报3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2起，学校内部自查事件2起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	8月13日	教育部漏洞报告平台通报学校某小程序存在逻辑漏洞问题	已整改
2	8月28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单位主机存在Ramnit蠕虫病毒问题	已整改
3	8月28日	教育部漏洞报告平台通报学校某单位信息系统存在信息泄露问题	已整改
4	8月30日	学校内部自查发现学校某单位信息系统存在敏感配置文件泄露问题	已整改
5	8月30日	学校内部自查发现某单位信息系统主页存在敏感信息泄露问题	已整改
6	8月31日	教育部漏洞报告平台通报某单位信息系统存在弱口令问题	已整改
7	8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某单位信息系统存在未授权访问问题	已整改

3、服务器受攻击情况

本次监测时间为8月，防火墙防护服务器受到攻击事件共1669602起；其中针对学校门户网站群系统的攻击次数达到127671起，占总数的7.64%。门户网站群系统提供我校221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	第二站群系统	127671
2	地球科学在线	87606
3	校园虚拟专用（VPN）网络	64036
4	远程教学学习管理系统	57662
5	研究生管理信息系统	41616

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：共发现中高危漏洞1084个，其中高危漏洞564个，中危漏洞520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	存在高危漏洞128个，中危漏洞103个
2	测试服务	存在高危漏洞49个，中危漏洞36个
3	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
4	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
5	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
6	档案应用系统	存在高危漏洞20个，中危漏洞0个
7	基建项目管理系统（BS）	存在高危漏洞13个，中危漏洞12个
8	基建项目管理系统（CS）	存在高危漏洞13个，中危漏洞12个
9	网络报修系统	存在高危漏洞10个，中危漏洞10个
10	中国地质大学（武汉）干部管理信息系统	存在高危漏洞9个，中危漏洞4个

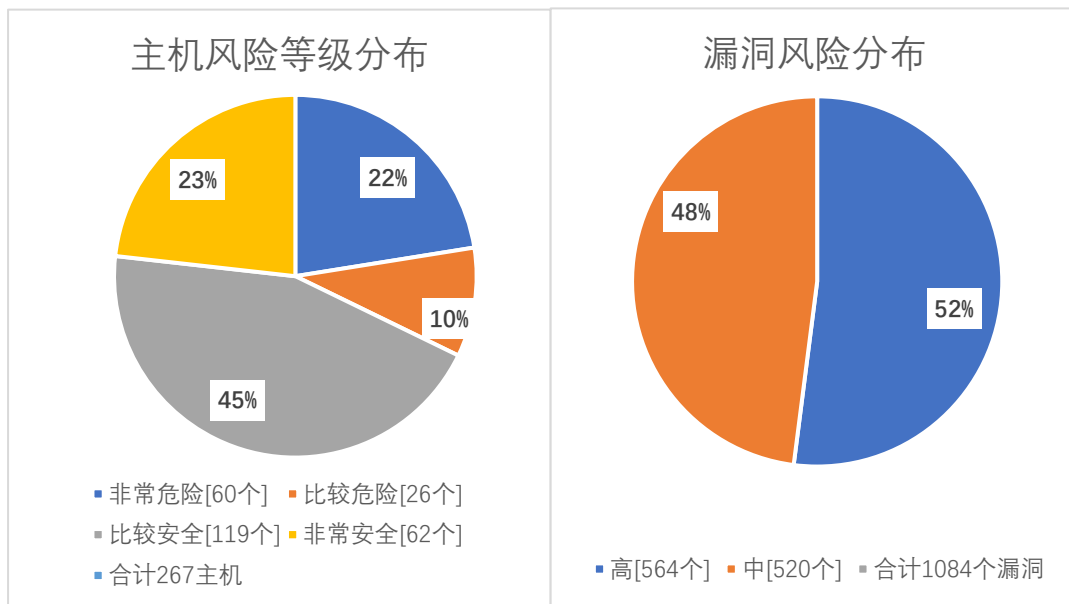
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

本月完成主机高危漏洞整改42个、主机中危漏洞整改40个。因备案系统增多及漏洞库更新，本月新增WEB中危漏洞4个。

本月漏洞数量较上月减少,9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,保证正常工作作用网安全。

漏洞数量	高危漏洞	中危漏洞	合计
8月	564	520	1084
7月	639	556	1195
变化量(个)	减少75个	减少36个	减少111个

在本月扫描的267台服务器中,主机、网站中高危漏洞总计1084个,其中高危漏洞564个,中危漏洞520个。主机风险等级中,非常危险的占22%,比较危险的占10%,比较安全的占45%,非常安全的占23%。漏洞风险等级中,高危漏洞占比52%,中危漏洞占比48%。



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)	40
高	Apache Tomcat 注入漏洞(CVE-2022-45143)	37
高	nginx 缓冲区错误漏洞(CVE-2022-41741)	29
高	nginx 越界写入漏洞(CVE-2022-41742)	29

高	Apache Tomcat 环境问题漏洞 (CVE-2022-42252)	20
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)	9