中国地质大学（武汉）网络安全月报

2024 年 9 月　（第 W00102 期）（发布）　总第 102 期

中国地质大学（武汉）信息化工作办公室　2024 年 9 月 30 日

1、情况综述

根据监测分析，9 月份我校校园网络发生的安全威胁事件共计 3404679 起。其中服务器受到攻击的事件 3404328 起、蠕虫病毒攻击事件 69 起、木马病毒攻击事件 282 起、来自外部的 DoS 攻击事件 0 起。

9 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，未发生重大的网络安全事件,后续会继续保持和完善。

2、安全事件通报

9 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事件 3 起，内部自查事件 6 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	9 月 2 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所属网络资产疑似遭境外黑客组织攻击控制	已整改
2	9 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某单位所属主机遭境外 APT 组织攻击	已整改
3	9 月 5 日	学校内部自查发现某网站存在暗链问题	已通报
4	9 月 5 日	学校内部自查发现某网站存在暗链问题	已通报
5	9 月 23 日	学校内部自查发现某网站存在暗链问题	已通报
6	9 月 23 日	学校内部自查发现某网站存在暗链问题	已通报
7	9 月 23 日	学校内部自查发现某网站存在暗链问题	已通报
8	9 月 24 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弱口令问题	已整改
9	9 月 26 日	学校内部自查发现某网站存在暗链问题	已整改

3、服务器受攻击情况

本次监测时间为 9 月，防火墙防护服务器受到攻击事件共 3404328 起；其中针对学校门户站群系统的攻击次数达到 27995 起，占总数的 0.83%。门户站群系统提供我校 192 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	校园虚拟专用网络（VPN）	1726691
2	机构知识库	389192
3	地球科学期刊官网	118062
4	校园一卡通平台	82758
5	珠宝学院	83150

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 434 个，中危漏洞 650 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	云因出版 ERP 管理系统	出版社	存在高危漏洞 42 个，中危漏洞 68 个。
2	海洋学院导师制管理系统	海洋学院	存在高危漏洞 41 个，中危漏洞 16 个。
3	人才信息系统	人力资源部	存在高危漏洞 40 个，中危漏洞 17 个。
4	未来城校区车辆门禁系统	未来城校区管理办公室	存在高危漏洞 33 个，中危漏洞 187 个。
5	档案应用系统	图书档案与文博部	存在高危漏洞 20 个，中危漏洞 0 个。
6	远程教学管理平台	远程与继续教育学院	存在高危漏洞 18 个，中危漏洞 4 个。
7	未来城校区综合管理展示平台	未来城校区管理办公室	存在高危漏洞 17 个，中危漏洞 9 个。
8	中国地质大学（武汉）图书馆微信	图书档案与文博部	存在高危漏洞 16 个，中危漏洞 34 个。
9	基建项目管理系统	校园规划与基建处	存在高危漏洞 13 个，中危漏洞 12 个。
10	金山论文管理系统	图书档案与文博部	存在高危漏洞 10 个，中危漏洞 20 个。

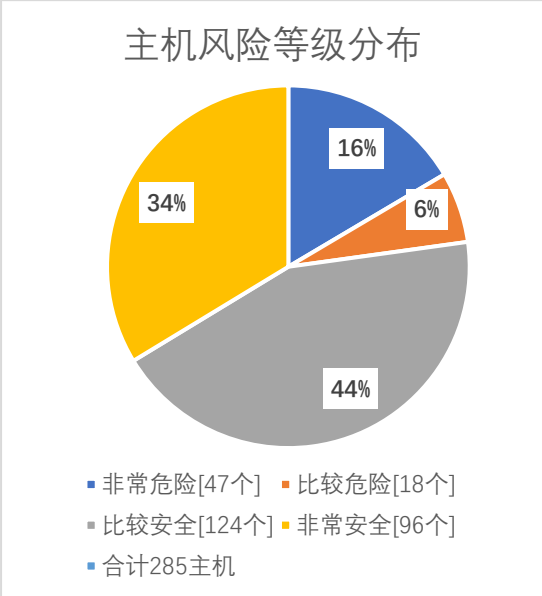
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

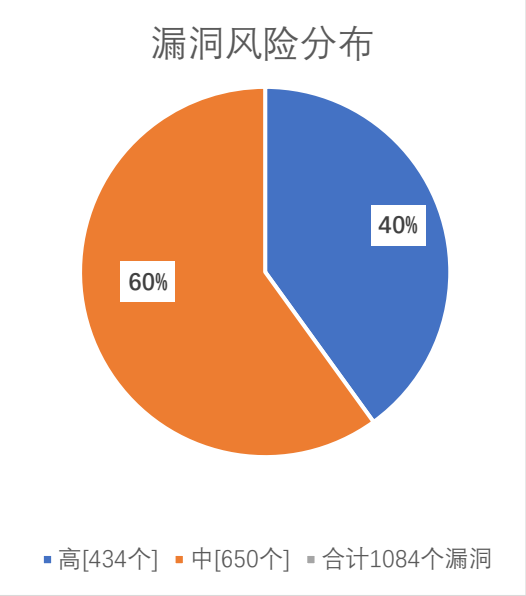
本月完成主机高危漏洞整改 20 个，主机中危漏洞整改 22 个；WEB 高危漏洞整改 3 个。因新业务上线及漏洞库更新，本月新增 WEB 中危漏洞 1 个。

本月漏洞数量较上月减少，10 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
9 月	434	650	1084
8 月	457	671	1128
变化量（个）	减少 23 个	减少 21 个	减少 44 个

在本月扫描的 285 台服务器中，主机、网站中高危漏洞总计 1084 个，其中高危漏洞 434 个，中危漏洞 650 个。主机风险等级中，非常危险的占 16%，比较危险的占 6%，比较安全的占 44%，非常安全的占 34%。漏洞风险等级中，高危漏洞占比 40%，中危漏洞占比 60%。





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 缓冲区错误漏洞(CVE-2022-41741)	27
高	nginx 越界写入漏洞（CVE-2022-41742）	27
高	Apache Tomcat 拒绝服务漏洞(CVE-2023-24998)	11
高	Apache Tomcat 注入漏洞(CVE-2022-45143)	9
高	Oracle MySQL zlib 安全漏洞(CVE-2022-37434)	7
高	Oracle MySQL 安全漏洞(CVE-2023-21912)	7
高	Oracle MySQL curl 安全漏洞(CVE-2022-43551)	7
高	Oracle MySQL 安全漏洞(CVE-2023-0215)	7
高	Oracle MySQL 安全漏洞(CVE-2023-21980)	7
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	6