中国地质大学（武汉）网络安全月报

2023 年 5 月　（第 W0086 期）　总第 86 期

中国地质大学（武汉）信息化工作办公室　2023 年 5 月 30 日

1、情况综述

根据监测分析，5 月份我校校园网络发生的安全威胁事件共计 356277 起。其中服务器受到攻击的事件 356195 起、蠕虫病毒攻击事件 10 起、木马病毒攻击事件 72 起、来自外部的 DoS 攻击事件 0 起。

5 月份我校总体网络安全情况良好，处理网络安全事件共 1 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

5 月处理网络安全事件共 1 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 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	5 月 17 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 5 月，防火墙防护服务器受到攻击事件共 356195 起；其中针对学校门户站群系统的攻击次数达到 38200 起，占总数的 10.72%。门户站群系统提供我校 214 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	129000
2	珠宝学院主页	96900
3	宝石和宝石学杂志	74400
4	图书馆主页	73800
5	机构知识库	60900

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：共发现中高危漏洞1034个，其中高危漏洞458个，中危漏洞576个，漏洞数量较上月基本持平。

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	高危漏洞121个，中危漏洞192个。
2	测试服务	高危漏洞39个，中危漏洞55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	基建项目管理系统（BS）	高危漏洞13个，中危漏洞12个。
7	一卡通平台_运维监控平台	高危漏洞11个，中危漏洞89个。
8	档案应用系统	高危漏洞10个，中危漏洞0个。
9	中国地质大学（武汉）干部管理信息系统	高危漏洞7个，中危漏洞3个。
10	远程与继续教育学院作业与考试系统	高危漏洞5个，中危漏洞35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27个、主机中危漏洞整改20个；WEB高危漏洞整改2个、WEB中危漏洞整改21个

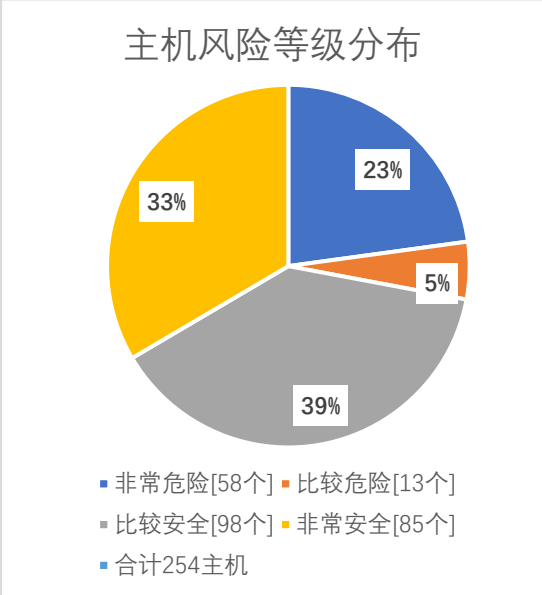
因新漏洞库更新，本月新增主机高危漏洞13个，主机中危漏洞62个。

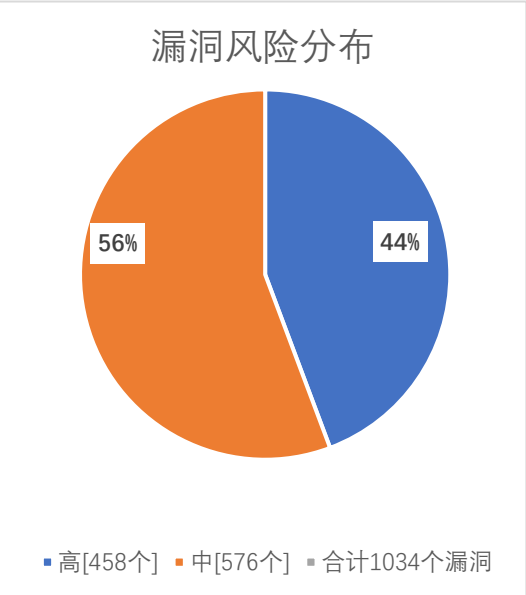
本月漏洞数量较上月基本持平，5月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	高危漏洞	中危漏洞	合计
5月	458	576	1034
4月	474	555	1029
变化量（个）	减少16个	增多21个	增多5个

在本月扫描的254台服务器中，主机、网站中高危漏洞总计1034个，其中高危漏洞458个，中危漏洞576个。主机风险等级中，非常危险的占23%，比较

危险的占 5%，比较安全的占 39%，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)	21
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	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	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	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