中国地质大学（武汉）网络安全月报

2023 年 3 月　（第 W0084 期）　总第 84 期

中国地质大学（武汉）信息化工作办公室　2023 年 3 月 31 日

1、情况综述

根据监测分析，3 月份我校校园网络发生的安全威胁事件共计 328425 起。其中服务器受到攻击的事件 328299 起、蠕虫病毒攻击事件 0 起、木马病毒攻击事件 126 起、来自外部的 DoS 攻击事件 0 起。

3 月份我校总体网络安全情况良好，处理网络安全事件共 2 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

3 月处理网络安全事件共 2 起。其中，教育部漏洞报告平台 2 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	3 月 21 日	教育部漏洞报告平台通报某信息系统存在系统软件设计漏洞问题	已整改
2	3 月 21 日	教育部漏洞报告平台通报某信息系统存在弱口令问题	已整改

3、服务器受攻击情况

本次监测时间为 2 月，防火墙防护服务器受到攻击事件共 328299 起；其中针对学校门户站群系统的攻击次数达到 106059 起，占总数的 32.25%。门户站群系统提供我校 184 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	站群系统	106059
2	校园虚拟专用（VPN）网络	27801

3	网上审批系统	11982
4	《宝石和宝石学杂志）》中英文网站	9066
5	地球科学在线	8499

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：共发现中高危漏洞1060个，其中高危漏洞462个，中危漏洞598个，漏洞数量较上月少量增加。

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	存在高危漏洞144个，中危漏洞253个。
2	测试服务	存在高危漏洞53个，中危漏洞39个。
3	商业门面从业人员管理系统	存在高危漏洞32个，中危漏洞24个。
4	海洋学院导师制管理系统	存在高危漏洞25个，中危漏洞14个。
5	中国地质大学（武汉）人才信息系统	存在高危漏洞24个，中危漏洞15个。
6	国际会议申报系统	存在高危漏洞24个，中危漏洞16个。
7	实验室安全巡检平台	存在高危漏洞15个，中危漏洞9个。
8	数据共享web网站	存在高危漏洞14个，中危漏洞6个。
9	基建项目管理系统（BS）	存在高危漏洞13个，中危漏洞12个。
10	一卡通平台_运维监控平台	存在高危漏洞11个，中危漏洞89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3个、主机中危漏洞整改47个、网站高危漏整改37个、网站中危漏洞整改25个。

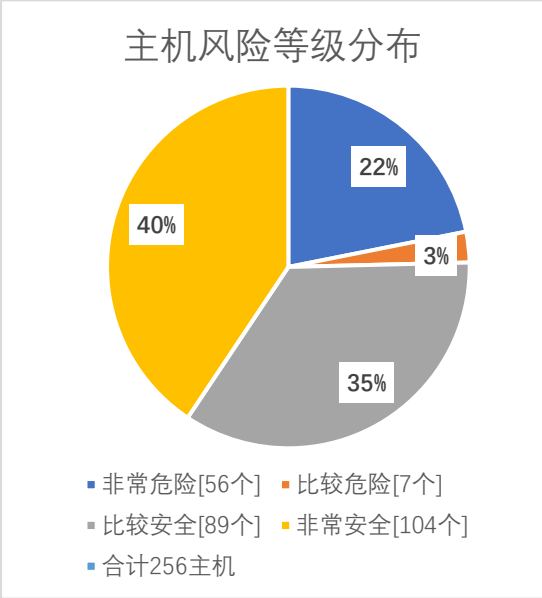
因新主机上线及漏洞库更新，本月新增主机高危漏洞57个，主机中危漏洞23个；新增网站高危漏洞17个，网站中危漏洞33个。

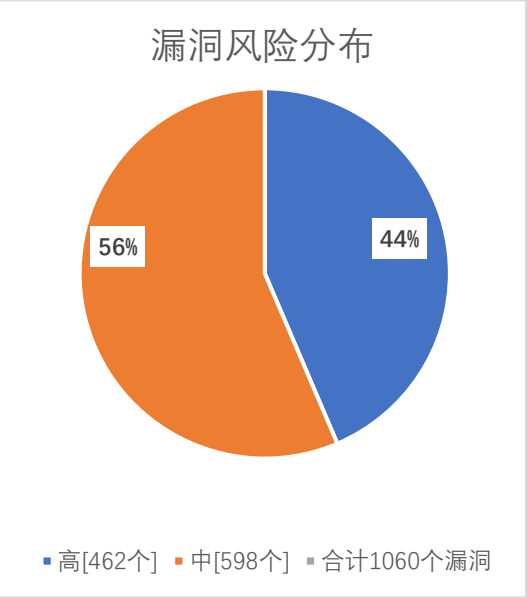
本月漏洞数量较上月少量增加，4月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	高危漏洞	中危漏洞	合计

3 月	462	598	1060
2 月	428	614	1042
变化量（个）	增多 34 个	减少 16 个	增多 18 个

在本月扫描的 256 台服务器中，主机、网站中高危漏洞总计 1060 个，其中高危漏洞 462 个，中危漏洞 598 个。主机风险等级中，非常危险的占 22%，比较危险的占 3%，比较安全的占 35%，非常安全的占 40%。漏洞风险等级中，高危漏洞占比 42%，中危漏洞占比 56%。





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)	23
高	Apache Tomcat 代码问题漏洞(CVE-2022-29885)	13
高	Eclipse Jetty 缓冲区错误漏洞(CVE-2009-5047)	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	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	11

高	nginx 安全漏洞(CVE-2021-23017)	10
高	Apache HTTP Server 缓冲区错误漏洞(CVE-2021-39275)	4
高	Apache 安全漏洞(CVE-2021-26691)	4