中国地质大学（武汉）网络安全月报

2024 年 2 月　（第 W0095 期）（发布）　总第 95 期

中国地质大学（武汉）信息化工作办公室　2024 年 2 月 29 日

1、情况综述

根据监测分析，2 月份我校校园网络发生的安全威胁事件共计 1053041 起。其中服务器受到攻击的事件 1051790 起、蠕虫病毒攻击事件 2 起、木马病毒攻击事件 1249 起、来自外部的 DoS 攻击事件 0 起。

2 月份我校总体网络安全情况良好，处理网络安全事件共 5 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

2 月处理网络安全事件共 5 起。其中教育漏洞报告平台通报事件 2 起，学校内部自查事件 3 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2 月 20 日	学校内部自查发现某网站存在暗链问题	已整改
2	2 月 22 日	教育部漏洞报告平台通报学校某信息系统存在源码泄露问题	已整改
3	2 月 22 日	教育部漏洞报告平台通报学校某信息系统存在越权、用户密码明文传输问题	已通报
4	2 月 27 日	学校内部自查发现某信息系统存在暗链问题	已整改
5	2 月 27 日	学校内部自查发现某网站存在暗链问题	已通报

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 1051790 起；其中针对学校门户站群系统的攻击次数达到 52549 起，占总数的 4.99%。门户站群系

统提供我校 190 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	科研管理系统	94800
2	地球科技通报	74370
3	校园虚拟专用网络	56279
4	站群系统	52549
5	研究生管理信息系统	24061

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 1048 个，其中高危漏洞 499 个，中危漏洞 549 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	东软数据中心	存在高危漏洞 49 个，中危漏洞 36 个。
2	云因出版 ERP 管理系统	存在高危漏洞 48 个，中危漏洞 73 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	人才信息系统	存在高危漏洞 40 个，中危漏洞 17 个。
6	校园一卡通平台	存在高危漏洞 26 个，中危漏洞 138 个。
7	远程教学管理平台	存在高危漏洞 23 个，中危漏洞 30 个。
8	档案应用系统	存在高危漏洞 20 个，中危漏洞 0 个。
9	未来城校区综合管理展示平台	存在高危漏洞 17 个，中危漏洞 9 个。
10	基建项目管理系统	存在高危漏洞 13 个，中危漏洞 12 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。

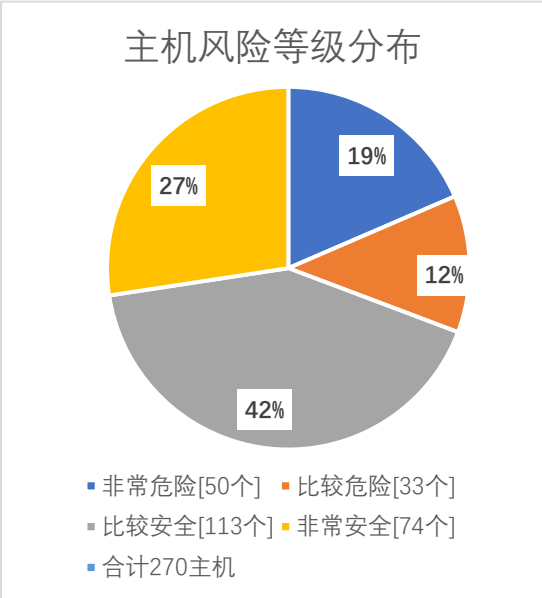
本月完成 WEB 中危漏洞整改 1 个。因漏洞库更新，本月新增主机高危漏洞 6 个，主机中危漏洞 7 个；新增 WEB 高危漏洞 6 个，WEB 中危漏洞 1 个。

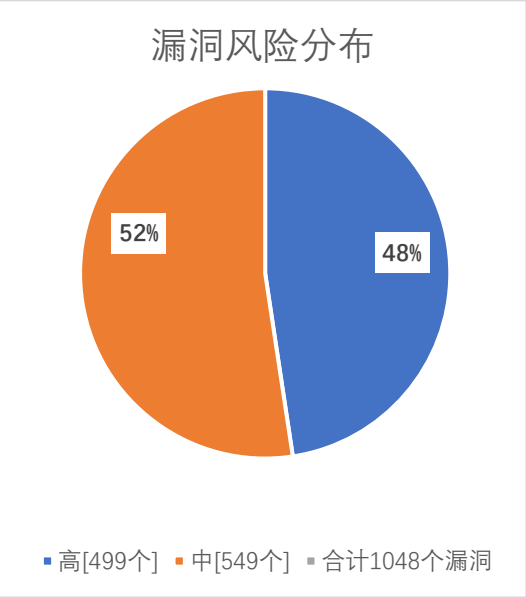
本月漏洞数量较上月少量增多，3 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	高危漏洞	中危漏洞	合计

2 月	499	549	1048
1 月	487	542	1029
变化量（个）	增加 12 个	增加 7 个	增加 19 个

在本月扫描的 270 台服务器中，主机、网站中高危漏洞总计 1048 个，其中高危漏洞 499 个，中危漏洞 459 个。主机风险等级中，非常危险的占 19%，比较危险的占 12%，比较安全的占 42%，非常安全的占 27%。漏洞风险等级中，高危漏洞占比 48%，中危漏洞占比 52%。





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)	19
高	Apache Tomcat 注入漏洞(CVE-2022-45143)	17
高	Apache Tomcat 安全漏洞(CVE-2023-28709)	10
高	Apache Tomcat 环境问题漏洞(CVE-2022-42252)	8
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	6

高	PHP 缓冲区错误漏洞(CVE-2022-31630)	6
高	Apache HTTP Server 环境问题漏洞(CVE-2023-25690)	4
高	Apache HTTP Server 安全漏洞(CVE-2022-36760)	4