中国地质大学（武汉）网络安全月报

2022 年 10 月　　（第 W0079 期）　　总第 79 期

中国地质大学（武汉）信息化工作办公室　　2022 年 11 月 01 日

1、情况综述

根据监测分析，10 月份我校校园网络发生的安全威胁事件共计 2121537 起。其中服务器受到攻击的事件 2114954 起、蠕虫病毒攻击事件 683 起、木马病毒攻击事件 350 起、来自外部的 DoS 攻击事件 5550 起。

10 月份我校总体网络安全情况良好，处理网络安全事件共 18 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

10 月处理网络安全事件共 18 起。其中，教育行业网络安全平台通报事件 14 起、学校自查通报事件 2 起、湖北省等保办公室通报事件 1 起、学生上报事件 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	10 月 3 日	教育行业网络安全平台通报某信息系统存在注入漏洞问题	已整改
2	10 月 3 日	教育行业网络安全平台通报某信息系统存在请求伪造漏洞问题	已整改
3	10 月 3 日	教育行业网络安全平台通报某信息系统存在访问控制及系统配置失效问题	已整改
4	10 月 3 日	教育行业网络安全平台通报某信息系统存在系统软件设计漏洞问题	已整改
5	10 月 3 日	教育行业网络安全平台通报某信息系统存在注入漏洞问题	已整改
6	10 月 3 日	教育行业网络安全平台通报某信息系统存在注入漏洞、双非网站问题	已督办
7	10 月 3 日	教育行业网络安全平台通报某信息系统存在注入漏洞问题	已关停
8	10 月 3 日	教育行业网络安全平台通报某安全设备存在系统软件设计漏洞问题	已整改

9	10 月 3 日	教育行业网络安全平台通报某信息系统存在系统软件设计漏洞、访问控制及系统配置失效、注入漏洞问题	已整改
10	10 月 3 日	教育行业网络安全平台通报某信息系统存在双非、系统软件设计漏洞、注入漏洞、请求伪造漏洞问题	已整改
11	10 月 3 日	教育行业网络安全平台通报某信息系统存在系统软件设计漏洞问题	已关停
12	10 月 3 日	教育行业网络安全平台通报某信息系统存在加密机制失效问题	已整改
13	10 月 10 日	教育行业网络安全平台通报某信息系统存在注入漏洞问题	已整改
14	10 月 10 日	教育行业网络安全平台通报某信息系统存在注入漏洞问题	已整改
15	10 月 10 日	学生上报发现某信息系统存在加密机制失效风险	已通报
16	10 月 19 日	学校自查发现某信息系统存在管理员弱口令漏洞问题	已整改
17	10 月 20 日	湖北省等保办公室通报某信息系统存在开源和商业应用框架漏洞的问题	已督办
18	10 月 27 日	学校内部自查发现某信息系统存在注入漏洞问题	已整改

3、服务器受攻击情况

本次监测时间为 10 月，防火墙防护服务器受到攻击事件共 2114954 起；其中针对学校门户站群系统的攻击次数达到 1046429 起，占总数的 49.48%。门户站群系统提供我校 185 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	1046429
2	教师个人主页发布系统	123594
3	地球科学在线	94516
4	校园虚拟专用（VPN）网络	51322

5	采购与招标信息管理系统	47453

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 1117 个，其中高危漏洞 344 个，中危漏洞 773 个，漏洞数量较上月明显减少。

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	云因出版 ERP 管理系统	存在高危漏洞 48 个，中危漏洞 73 个
2	高性能计算公共服务平台	存在高危漏洞 39 个，中危漏洞 50 个
3	检测查询网站	存在高危漏洞 33 个，中危漏洞 44 个
4	远程教学大数据集群	存在高危漏洞 8 个，中危漏洞 6 个
5	商业门面从业人员管理系统	存在高危漏洞 6 个，中危漏洞 4 个
6	学生请假预约系统	存在高危漏洞 6 个，中危漏洞 4 个
7	容器云管理平台	存在高危漏洞 3 个，中危漏洞 3 个
8	中国地质大学资产综合管理系统	存在高危漏洞 3 个，中危漏洞 5 个
9	校园一卡通平台	存在高危漏洞 3 个，中危漏洞 5 个
10	远程教学大数据集群	存在高危漏洞 2 个，中危漏洞 3 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 324 个、主机中危漏洞整改 539 个、网站高危漏整改 61 个、网站中危漏洞整改 141 个。

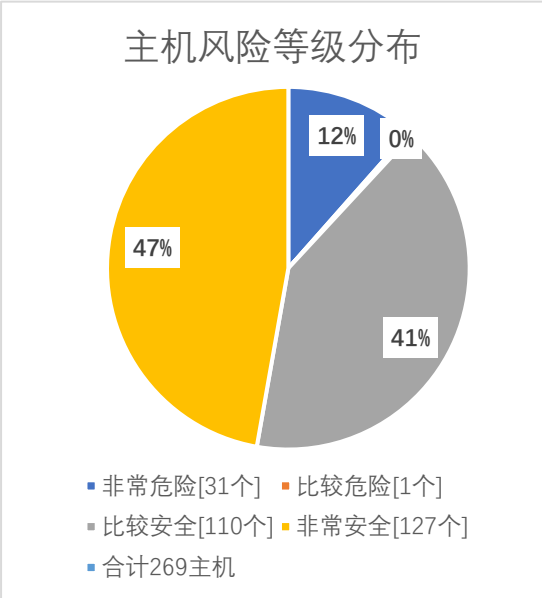
因漏洞库更新，本月新增主机高危漏洞 144 个，主机中危漏洞 470 个；新增网站高危漏洞 24 个，网站中危漏洞 62 个。

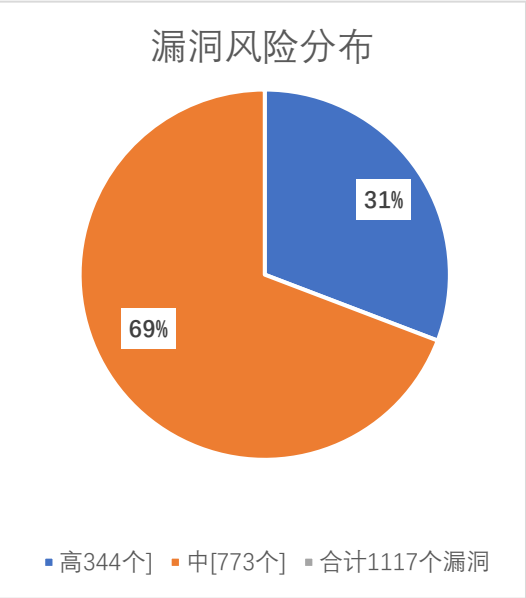
本月漏洞数量较上月明显减少，11 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	高危漏洞	中危漏洞	合计
10 月	344	773	1117

9 月	561	921	1482
变化量（个）	减少 217	减少 148	减少 365

在本月扫描的 269 台服务器中，主机、网站中高危漏洞总计 1117 个，其中高危漏洞 344 个，中危漏洞 773 个。主机风险等级中，非常危险的占 12%，比较危险的占 0%，比较安全的占 41%，非常安全的占 47%。漏洞风险等级中，高危漏洞占比 31%，中危漏洞占比 69%。





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	Eclipse Jetty 安全漏洞(CVE-2020-27216)	9
高	Eclipse Jetty 缓冲区错误漏洞(CVE-2009-5047)	8
高	Eclipse Jetty Dump Servlet 信息泄露漏洞(CVE-2009-5045)	8
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	7
高	检测到远端 X 服务正在运行中(CVE-1999-0526)	6
高	nginx 安全漏洞(CVE-2021-23017)	4
高	PHP 远程命令执行漏洞(CVE-2022-31625)	3
高	Apache Tomcat 代码问题漏洞(CVE-2022-29885)	3

高	Oracle MySQL/MariaDB Packaging (OpenSSL)全漏洞(CVE-2022-0778)	3
高	目标主机 showmount -e 信息泄露(CVE-1999-0554)	2