# 中国地质大学（武汉）网络安全月报

2022 年 6 月　（第 W0076 期）　总第 76 期

中国地质大学（武汉）信息化工作办公室　2022 年 6 月 30 日

## 1、情况综述

根据监测分析，6 月份我校校园网络发生的安全威胁事件共计 1201687 起，其中服务器受到攻击的事件共计 626188 起；网站受到攻击的事件共计 575499 起；可能感染病毒木马的僵尸主机共 5 台，其中确定的僵尸主机共 2 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

6 月份我校总体网络安全情况良好，处理网络安全事件共 23 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

6 月处理网络安全事件共 23 起。学校自查通报事件 23 起。

**网络安全事件汇总表**

| 序号 | 时间 | 内容 | 处理结果 |
|---|---|---|---|
| 1 | 6月3日 | 学校内部自查发现某信息系统存在双非网站、文件上传漏洞问题 | 已整改 |
| 2 | 6月3日 | 学校内部自查发现某信息系统存在存储型XSS漏洞和远程代码执行漏洞问题 | 已整改 |
| 3 | 6月4日 | 学校内部自查发现某信息系统存在暗链问题 | 已整改 |
| 4 | 6月10日 | 学校内部自查发现某信息系统存在phpinfo信息泄露问题 | 已整改 |
| 5 | 6月10日 | 学校内部自查发现某信息系统存在Druid未授权访问问题 | 已整改 |
| 6 | 6月10日 | 学校内部自查发现某信息系统存在Druid未授权访问问题 | 已整改 |
| 7 | 6月17日 | 学校内部自查发现某信息系统存在服务器弱口令问题 | 已整改 |
| 8 | 6月17日 | 学校内部自查发现某信息系统存在敏感信息问题 | 已整改 |
| 9 | 6月17日 | 学校内部自查发现某信息系统存在目录遍历问题 | 已整改 |

| | | | |
|---|---|---|---|
| 10 | 6月17日 | 学校内部自查发现某信息系统存在重装问题 | 已整改 |
| 11 | 6月17日 | 学校内部自查发现某信息系统存在未授权访问问题 | 已整改 |
| 12 | 6月18日 | 学校内部自查发现某信息系统存在信息泄漏问题 | 已整改 |
| 13 | 6月18日 | 学校内部自查发现某信息系统存在信息泄漏问题 | 已整改 |
| 14 | 6月18日 | 学校内部自查发现某信息系统存在目录遍历问题 | 已整改 |
| 15 | 6月18日 | 学校内部自查发现某信息系统存在信息泄漏问题 | 已整改 |
| 16 | 6月18日 | 学校内部自查发现某信息系统存在信息泄漏问题 | 已整改 |
| 17 | 6月21日 | 学校内部自查发现某信息系统存在SQL注入漏洞问题 | 已整改 |
| 18 | 6月21日 | 学校内部自查发现某服务器存在服务器ssh弱口令问题 | 已整改 |
| 19 | 6月21日 | 学校内部自查发现某信息系统存在弱口令问题 | 已整改 |
| 20 | 6月21日 | 学校内部自查发现某信息系统存在反射性XSS问题 | 已整改 |
| 21 | 6月21日 | 学校内部自查发现某信息系统存在未加密传输问题 | 已整改 |
| 22 | 6月21日 | 学校内部自查发现某信息系统存在文件上传漏洞问题 | 已整改 |
| 23 | 6月21日 | 学校内部自查发现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 6 月，防火墙防护服务器受到攻击事件共 626188 起；其中针对学校门户站群系统的攻击次数达到 105608 起，占总数的 16.87%。门户站群系统提供我校 185 个各类网站的管理、发布功能，可以有效防护攻击，保障网站安全。

受攻击次数排名前十的服务器列表

| 序号 | 目标服务器 IP/名称 | 攻击次数 | 百分比 |
|---|---|---|---|
| 1 | 教师个人主页发布系统 | 140916 | 22.50% |
| 2 | 第一站群系统 | 105608 | 16.87% |
| 3 | 地球科学在线 | 47518 | 7.59% |
| 4 | 校园网 VPN 服务 | 32077 | 5.12% |
| 6 | 中国地质大学珠宝学院 | 25609 | 4.09% |
| 5 | 第二站群系统 | 17475 | 2.79% |
| 7 | 检测数据查询 | 12474 | 1.99% |
| 9 | 宝石和宝石学杂志 | 10294 | 1.64% |
| 10 | 图书馆主页 | 9989 | 1.60% |
| 8 | 财务与资产管理部 | 9840 | 1.57% |
| 12 | 其他 | 214388 | 34.24% |
| 13 | 所有 | 626188 | 100.00% |

## 4、服务器漏洞扫描分析

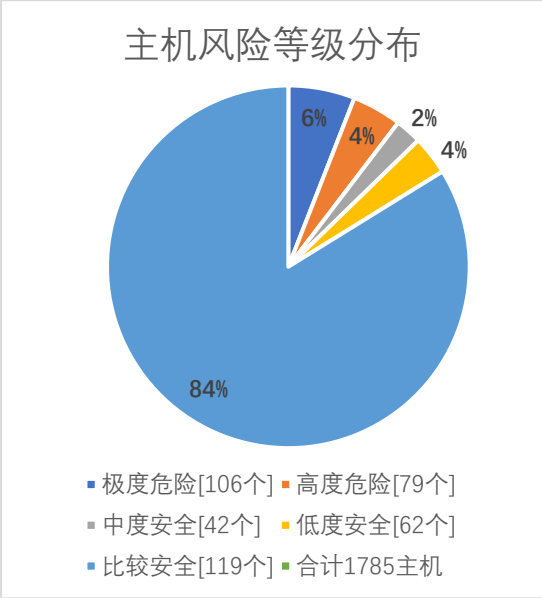
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 796 个，中危漏洞 3791 个，低危漏洞 4816 个，漏洞数量较上月明显增多。

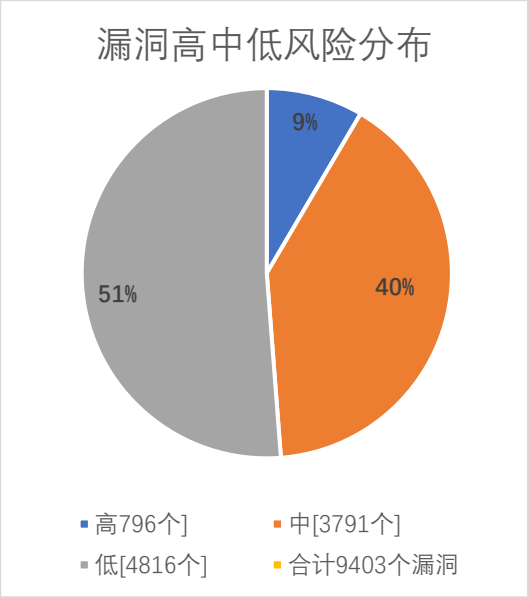
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

本月漏洞数量较上月明显增多，7 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 | 主机高危 | 主机中危 | 主机低危 | 合计 |
|---|---|---|---|---|
| 6 月 | 796 | 3791 | 4816 | 9403 |
| 5 月 | 874 | 3844 | 3580 | 8298 |
| 变化量（个） | 减少 78 | 减少 53 | 增加 1236 | 增加 1105 |

在本月扫描的 1785 台服务器中，主机漏洞总计 9403 个，其中高危漏洞 796 个，中危漏洞 3791 个，低危漏洞 4816 个。主机风险等级中，极度危险的占 6%，高度危险的占 4%，中度危险的占 2%，低度危险的占 4%，比较安全占 84%。漏洞风险等级中，高危漏洞占比 9%，中危漏洞占比 40%，低危漏洞占比 51%。




**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 | OpenSSH 安全漏洞(CVE-2016-10009) | 16 |
| 高 | OpenSSH sshd 安全漏洞(CVE-2016-6515) | 16 |
| 高 | OpenSSH sshd 安全漏洞(CVE-2015-8325) | 16 |
| 高 | OpenSSH 安全漏洞(CVE-2016-10012) | 16 |
| 高 | penSSH'ssh/kex.c'拒绝服务漏洞(CVE-2016-8858) | 16 |
| 高 | OpenSSH 安全漏洞(CVE-2016-1908) | 14 |
| 高 | Microsoft CredSSP 安全漏洞(CVE-2018-0886)[原理扫描] | 14 |
| 高 | Microsoft Windows RDP 协议安全漏洞（CVE-2019-0708）[原理扫描] | 14 |
| 高 | OpenSSH sshd 权限许可和访问控制漏洞 CVE-2015-5600 | 14 |

| | | |
|---|---|---|
| 高 | Microsoft Windows SMB 输入验证漏洞(CVE-2017-0144)(方程式工具-永恒之蓝)[原理扫描] | 12 |

## 5、安全漏洞整改情况

6 月信息化工作办公室针对安全漏洞给出了具体的整改建议。有重点分批次通知各服务器或应用系统所属部门系统管理员，按照漏洞危险程度逐步完成整改。相比于 5 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 1343 种，web 漏洞类型增多 22 种。6 月发放漏洞整改通知书 87 份，完成 11 个信息系统复检，总计 16 次。

对比 5 月，本月高危漏洞个数减少 78 个，总的漏洞数量增加 1105 个。

信息化工作办公室一直对受攻击较严重的服务器进行重点关注，并通知到所受单位服务器系统管理员。对于危险性较高的漏洞特别是应用系统漏洞，及时发现及时通知系统管理员整改。

校园网络内部安全隐患比较严重，全校应在网络安全管理和意识方面引起足够重视。