# 中国地质大学（武汉）网络安全月报

2021 年 10 月　　（第 W0068 期）　　总第 68 期

中国地质大学（武汉）信息化工作办公室　　2021 年 10 月 31 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 1410036 起，其中服务器受到攻击的事件共计 761674 起；网站受到攻击的事件共计 648362 起；可能感染病毒木马的僵尸主机共 10 台，其中确定的僵尸主机共 10 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 1 个。

10 月份我校总体网络安全情况良好，处理网络安全事件共 3 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 3 起。其中教育行业漏洞报告平台通报事件 3 起。

**网络安全事件汇总表**

| 序号 | 时间 | 内容 | 处理结果 |
|---|---|---|---|
| 1 | 10 月 22 号 | 教育行业漏洞报告平台通报我校某信息系统存在弱口令、敏感信息泄露问题 | 已整改 |
| 2 | 10 月 22 号 | 教育行业漏洞报告平台通报我校某信息系统存在弱口令问题 | 已整改 |
| 3 | 10 月 22 号 | 教育行业漏洞报告平台通报我校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 10 月，防火墙防护服务器受到攻击事件共 761674 起；其中针对学校门户站群系统的攻击次数达到 206877 起，占总数的 27.16%。门户站群系统提供我校 176 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 | 第一站群系统 | 206877 | 27.16% |
| 2 | 教师个人主页发布系统 | 86823 | 11.40% |
| 3 | 地球科学在线 | 55637 | 7.30% |
| 4 | 第二站群系统 | 49996 | 6.56% |
| 5 | 校园网 VPN 服务 | 39001 | 5.12% |
| 6 | 地质科技情报 | 25801 | 3.39% |
| 7 | 中国地质大学出版社有限责任公司 | 16484 | 2.16% |
| 8 | 中国地质大学珠宝学院 | 13659 | 1.79% |
| 9 | 检测数据查询 | 11320 | 1.49% |
| 10 | 校外访问平台 | 11080 | 1.45% |
| 11 | 其他 | 244996 | 32.17% |
| 12 | 所有 | 761674 | 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：共发现高危漏洞1227种，中危漏洞1668种，低危漏洞369种，漏洞种类较上月明显增多。

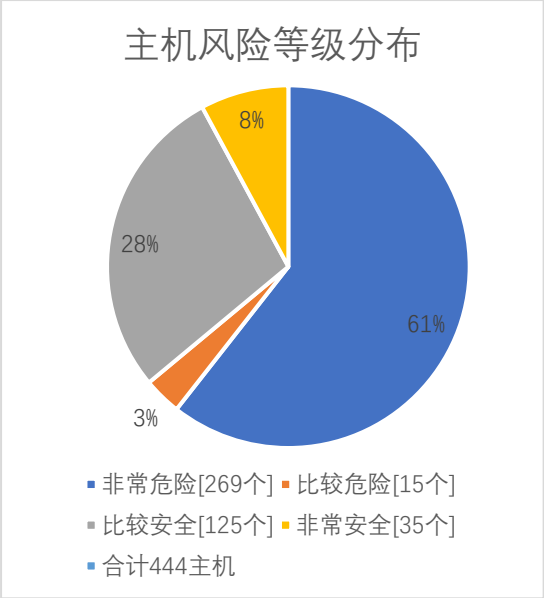
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

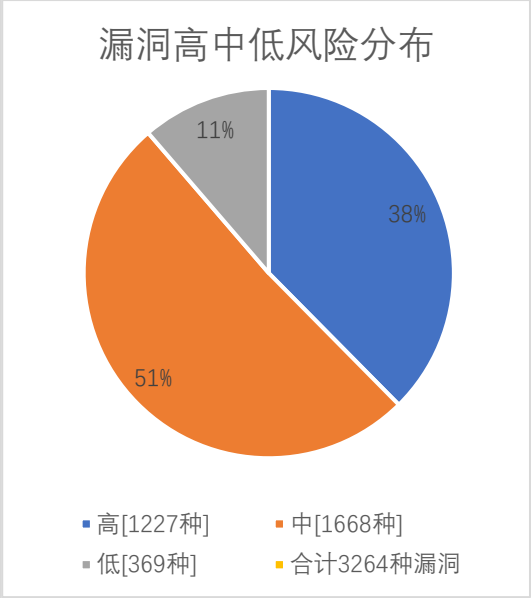
本月漏洞数量较上月明显增多，11月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

| 漏洞数量 | 主机高危 | 主机中危 | 主机低危 | 合计 |
|---|---|---|---|---|
| 10月 | 3573 | 4450 | 3706 | 11729 |
| 9月 | 1594 | 2314 | 2341 | 6249 |
| 变化量（个） | +1979 | +2136 | +1365 | +5480 |

| 漏洞种类 | 主机高危 | 主机中危 | 主机低危 | 合计 |
|---|---|---|---|---|
| 10月 | 1227 | 1668 | 369 | 3264 |
| 9月 | 504 | 941 | 267 | 1712 |
| 变化量（种） | +723 | +727 | +102 | +1552 |

在本月扫描的444台服务器中，主机漏洞3264种，主机漏洞总计11729个，其中高危漏洞1227种，总计3573个；中危漏洞1668种，总计4450个；低危漏洞369，总计3706个。主机风险等级中，非常危险的占61%，比较危险的占3%，比较安全的占28%，非常安全的占8%。漏洞风险等级中，高危漏洞占比38%，中危漏洞占比51%，低危漏洞占比11%。




**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 | CentOS GNOME libsoup 安全漏洞(CVE-2018-12910) | 226 |
| 高 | OpenSSH 命令注入漏洞(CVE-2020-15778) | 132 |
| 高 | SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】 | 92 |
| 高 | CentOS libXcursor 安全漏洞(CVE-2015-9262) | 56 |
| 高 | OpenSSH 安全限制绕过漏洞(CVE-2016-10012) | 55 |
| 高 | OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325) | 55 |
| 高 | OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515) | 55 |
| 高 | OpenSSH 多个拒绝服务漏洞（CVE-2016-10708） | 55 |
| 高 | OpenSSH 远程代码执行漏洞(CVE-2016-10009) | 55 |
| 高 | CentOS libqt5-qtbase 安全漏洞(CVE-2018-19873) | 54 |

## 5、安全漏洞整改情况

10 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 9 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 5214 种，web 漏洞类型增多 10 种。10 月发放漏洞整改通知书 88 份，完成 7 个信息系统复检，总计 7 次。

对比 9 月，本月高危漏洞类型增多 723 种，高危漏洞个数增多 1979 个，总的漏洞类型增多 1552 种，总的漏洞数量增多 5480 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。