中国地质大学（武汉）网络安全月报

2022 年 4 月　（第 W0074 期）　总第 74 期

中国地质大学（武汉）信息化工作办公室　2022 年 4 月 30 日

1、情况综述

根据监测分析，4 月份我校校园网络发生的安全威胁事件共计 1292962 起，其中服务器受到攻击的事件共计 704223 起；网站受到攻击的事件共计 588739 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 8 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

4 月份我校总体网络安全情况良好，处理网络安全事件共 11 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

4 月处理网络安全事件共 11 起。其中教育行业漏洞报告平台通报事件 4 起，教育系统网络安全工作管理平台安全监测预警子系统通报事件 3 起，上级部门通报事件 2 起，学校网络安全团队通报事件 1 起，湖北省网络与信息安全信息通报中心通报事件 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	4月7日	上级部门通报我校某信息系统存在双非网站问题	已整改
2	4月7日	上级部门通报我校某信息系统存在双非网站问题	已整改
3	4月12日	学校网络安全团队通报我校某信息系统存在页面被恶意篡改问题	已整改
4	4月19日	教育行业漏洞报告平台通报我校某信息系统存在敏感信息泄露问题	已整改
5	4月19日	教育行业漏洞报告平台通报我校某信息系统存在SSRF安全漏洞问题	已整改
6	4月19日	教育行业漏洞报告平台通报我校某信息系统存在逻辑漏洞问题	已整改
7	4月19日	教育行业漏洞报告平台通报我校某信息系统存在逻辑漏洞问题	已整改

8	4月26日	湖北省网络与信息安全信息通报中心通报我校某信息系统存在弱口令问题	已整改
9	4月29日	教育系统网络安全工作管理平台安全监测预警子系统通报我校某信息系统存在未授权访问问题	已整改
10	4月29日	教育系统网络安全工作管理平台安全监测预警子系统通报我校某信息系统存在暗链问题	已整改
11	4月29日	教育系统网络安全工作管理平台安全监测预警子系统通报我校某信息系统存在远程执行命令漏洞问题	已整改

3、服务器受攻击情况

本次监测时间为 4 月，防火墙防护服务器受到攻击事件共 704223 起；其中针对学校门户站群系统的攻击次数达到 104255 起，占总数的 14.80%。门户站群系统提供我校 184 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	145655	20.68%
2	第一站群系统	104255	14.80%
3	地球科学在线	47453	6.74%
4	校园网 VPN 服务	37797	5.37%
5	中国地质大学珠宝学院	20645	2.93%
6	第二站群系统	18123	2.57%
7	中国地质大学出版社有限责任公司	15684	2.23%
8	宝石和宝石学杂志	10791	1.53%
9	图书馆主页	9904	1.41%
10	财务与资产管理部	9797	1.39%
11	其他	284119	40.35%
12	所有	704223	100.00%

4、服务器漏洞扫描分析

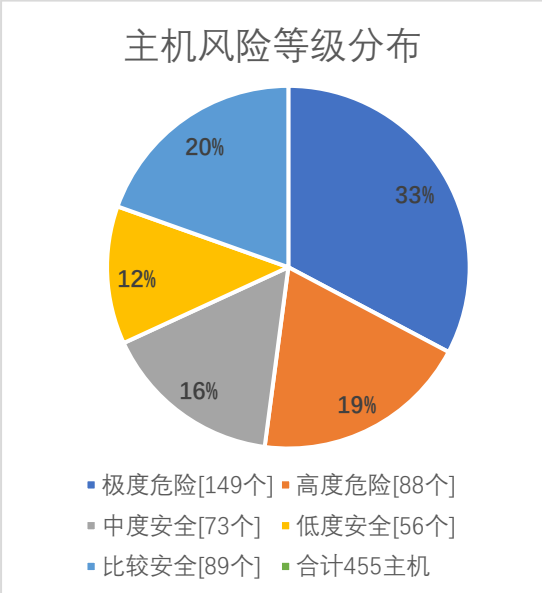
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1380 个，中危漏洞 5802 个，低危漏洞 4426 个，漏洞数量较上月明显增多。

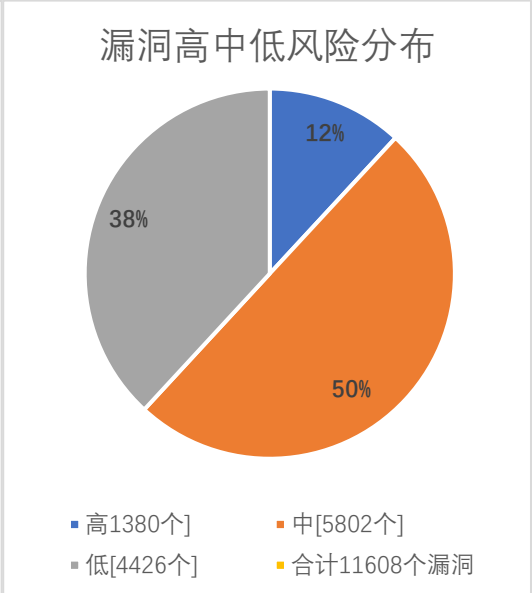
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

本月漏洞数量较上月明显增多，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	主机高危	主机中危	主机低危	合计
4 月	1380	5802	4426	11608
3 月	1231	5346	4527	11104
变化量（个）	增加 146	增加 456	减少 101	增加 504

在本月扫描的 455 台服务器中，主机漏洞总计 11608 个，其中高危漏洞 1380 个；中危漏洞 5802 个；低危漏洞 4426 个。主机风险等级中，极度危险的占 33%，高度危险的占 29%，中度危险的占 16%，低度危险的占 14%，比较安全占 20%。漏洞风险等级中，高危漏洞占比 12%，中危漏洞占比 50%，低危漏洞占比 38%。





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 sshd 安全漏洞(CVE-2015-8325)	37
高	OpenSSH'ssh/kex.c'拒绝服务漏洞(CVE-2016-8858)	37
高	OpenSSH 安全漏洞(CVE-2016-10009)	37
高	OpenSSH sshd 安全漏洞(CVE-2016-6515)	37
高	OpenSSH 安全漏洞(CVE-2016-10012)	37
高	OpenSSH 安全漏洞(CVE-2016-1908)	34
高	OpenSSH sshd 权限许可和访问控制漏洞 CVE-2015-5600	34
高	OpenSSH‘hash_buffer’函数缓冲区溢出漏洞(CVE-2014-1692)	31
高	OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478)	21
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]	20

5、安全漏洞整改情况

4 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 3 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 1241 种，web 漏洞类型增多 46 种。4 月发放漏洞整改通知书 63 份，完成 5 个信息系统复检，总计 11 次。

对比 3 月，本月高危漏洞个数增多 146 个，总的漏洞数量增多 504 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。