中国地质大学（武汉）网络安全月报

2022 年 5 月　（第 W0075 期）　总第 75 期

中国地质大学（武汉）信息化工作办公室　2022 年 5 月 31 日

1、情况综述

根据监测分析，5 月份我校校园网络发生的安全威胁事件共计 1091857 起，其中服务器受到攻击的事件共计 601972 起；网站受到攻击的事件共计 489885 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 7 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

5 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

5 月处理网络安全事件共 13 起。其中教育部通报事件 13 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	5月5日	教育部通报我校某信息系统存在暗链问题	已整改
2	5月14日	教育部通报我校某信息系统存在弱密码、信息泄露问题	已整改
3	5月15日	教育部通报我校某信息系统存在shiro反序列化漏洞存在Shiro 反序列化漏洞问题	已整改
4	5月19日	教育部通报我校某信息系统存在逻辑漏洞问题	已整改
5	5月20日	教育部通报我校某信息系统存在弱口令问题	已整改
6	5月21日	教育部通报我校某信息系统存在未授权、弱口令问题	已整改
7	5月21日	教育部通报我校某信息系统存在任意文件上传、敏感信息泄露问题	已整改
8	5月22日	教育部通报我校某信息系统存在弱口令问题	已整改
9	5月22日	教育部通报我校某些系统存在敏感信息泄露、任意文件上传漏洞、弱口令、shiro反序列化漏洞、逻辑漏洞	已整改

		等问题	
10	5月23日	教育部通报我校某系统存在弱口令问题	已整改
11	5月23日	教育部通报我校某系统存在文件遍历漏洞问题	已整改
12	5月23日	教育部通报我校某系统存在弱口令、任意文件上传漏洞问题	已整改
13	6月1日	教育部通报我校某网站存在暗链问题	已整改

3、服务器受攻击情况

本次监测时间为 5 月，防火墙防护服务器受到攻击事件共 601972 起；其中针对学校门户站群系统的攻击次数达到 62635 起，占总数的 10.40%。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	85761	14.25%
2	第一站群系统	62635	10.40%
3	地球科学在线	44422	7.38%
4	校园网 VPN 服务	21688	3.60%
5	第二站群系统	15532	2.58%
6	中国地质大学珠宝学院	12403	2.06%
7	检测数据查询	8736	1.45%
8	财务与资产管理部	8656	1.44%
9	远程与继续教育学院作业与考试系统	8450	1.40%
10	珠宝学院职教中心	7225	1.20%
12	其他	326464	54.23%
13	所有	601972	100.00%

4、服务器漏洞扫描分析

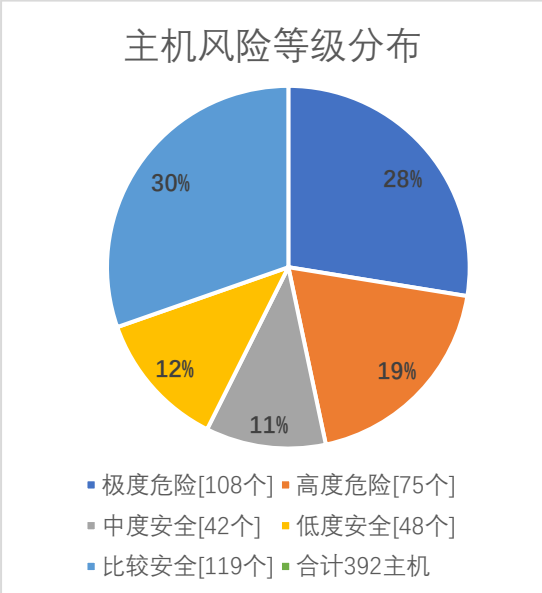
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 874 个，中危漏洞 3844 个，低危漏洞 3580 个，漏洞数量较上月明显减少。

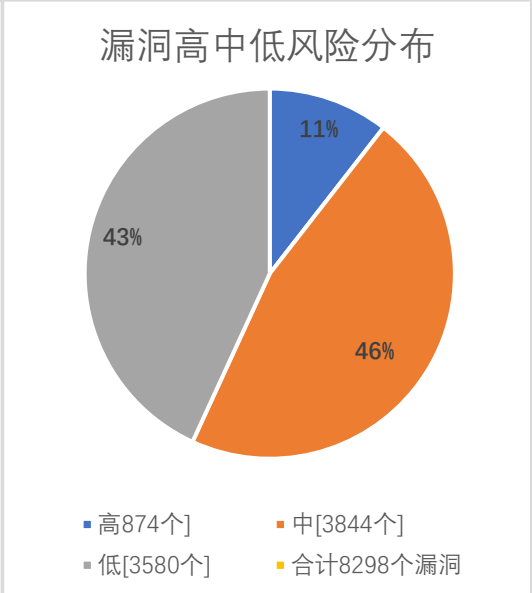
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

本月漏洞数量较上月明显增多，6 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
5 月	874	3844	3580	8298
4 月	1380	5802	4426	11608
变化量（个）	减少 506	减少 1958	减少 846	减少 3310

在本月扫描的 392 台服务器中，主机漏洞总计 8298 个，其中高危漏洞 874 个，中危漏洞 3844 个，低危漏洞 3580 个。主机风险等级中，极度危险的占 28%，高度危险的占 19%，中度危险的占 11%，低度危险的占 12%，比较安全占 30%。漏洞风险等级中，高危漏洞占比 11%，中危漏洞占比 46%，低危漏洞占比 43%。





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)	26
高	OpenSSH'ssh/kex.c'拒绝服务漏洞(CVE-2016-8858)	26
高	OpenSSH 安全漏洞(CVE-2016-10009)	26
高	OpenSSH sshd 安全漏洞(CVE-2016-6515)	26
高	OpenSSH 安全漏洞(CVE-2016-10012)	26
高	OpenSSH 安全漏洞(CVE-2016-1908)	24
高	OpenSSH sshd 权限许可和访问控制漏洞 CVE-2015-5600	24
高	OpenSSH‘hash_buffer’函数缓冲区溢出漏洞(CVE-2014-1692)	20
高	OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478)	16
高	Microsoft CredSSP 安全漏洞(CVE-2018-0886)[原理扫描]	13

5、安全漏洞整改情况

5 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 4 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 1602 种，web 漏洞类型增多 42 种。5 月发放漏洞整改通知书 67 份，完成 18 个信息系统复检，总计 26 次。

对比 4 月，本月高危漏洞个数减少 506 个，总的漏洞数量减少 3310 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。