中国地质大学（武汉）网络安全月报

2021 年 05 月　　（第 W0063 期）　总第 63 期

中国地质大学（武汉）网络与信息中心　　2021 年 05 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 1176974 起，其中服务器受到攻击的事件共计 626633 起；网站受到攻击的事件共计 550341 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。

5 月份我校总体网络安全情况良好，处理网络安全事件共 6 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 6 起。其中教育行业漏洞报告平台通报事件 6 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	5 月 6 日	教育行业漏洞报告平台通报我校数某单位用户存在遍历，未授权访问漏洞	已整改
2	5 月 12 日	教育行业漏洞报告平台通报我校某系统存在弱口令漏洞	已整改
3	5 月 12 日	教育行业漏洞报告平台通报我校某平台存在弱密码、任意文件上传漏洞	已整改
4	5 月 23 日	教育行业漏洞报告平台通报我校某平台存在网页 session 泄露问题	已整改
5	5 月 24 日	教育行业漏洞报告平台通报我校某平台存在弱口令、敏感信息泄露问题	已整改
6	5 月 25 日	教育行业漏洞报告平台通报我校某系统存在敏感信息泄露问题	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 626633 起；其中针对学校门户站群系统的攻击次数达到 121936 起，占总数的 19.46%。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	121936	19.46%
2	教师个人主页发布系统	86360	13.78%
3	地球科学在线	64287	10.26%
4	校园网 VPN 服务	32715	5.22%
5	第二站群系统	17740	2.83%
6	中国地质大学出版社有限责任公司	16937	2.70%
7	图书馆主页	15352	2.45%
8	地质科技情报	13276	2.12%
9	机构知识库	12103	1.93%
10	检测数据查询	9421	1.50%
11	其他	236506	37.74%
12	所有	626633	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 种，中危漏洞 1488 种，低危漏洞 321 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。网络与信息中心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，整改后上报网络与信息中心进行复检。

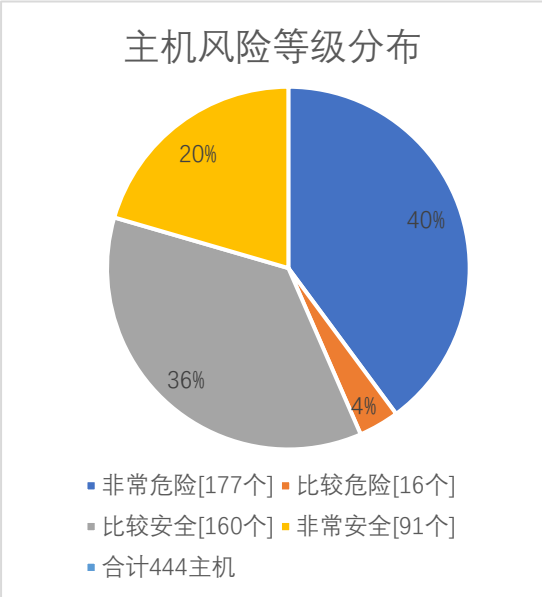
本月漏洞数量较上月增多，6 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

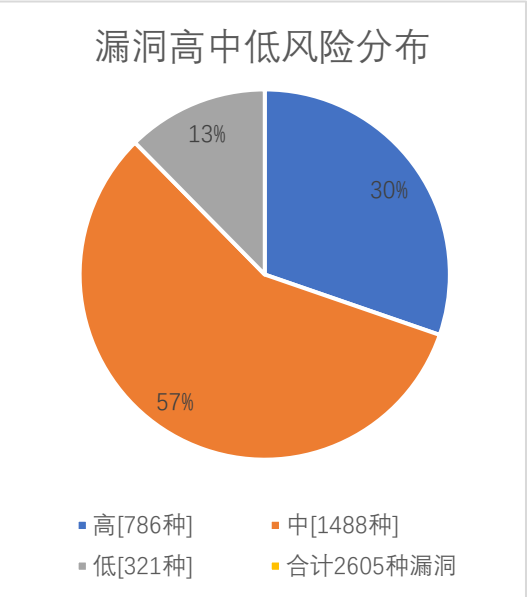
漏洞数量	主机高危	主机中危	主机低危	合计
4 月	2403	4691	3166	10260
5 月	2992	4399	2928	10319
变化量（个）	+589	-292	-238	+59

漏洞种类	主机高危	主机中危	主机低危	合计
4 月	742	1465	337	2544
5 月	796	1488	321	2605
变化量（种）	+54	+23	-16	+61

在本月扫描的 444 台服务器中，主机漏洞 22605 种，主机漏洞总计 10319 个，其中高危漏洞 796 种，总计 2992 个；中危漏洞 1488 种，总计 4399 个；低危漏洞 321，总计 2928 个。主机风险等级中，非常危险的占 40%，比较危险的占 4%，比较安全的占 36%，非常安全的占 20%。漏洞风险等级中，高危漏洞占

比 30%，中危漏洞占比 57%，低危漏洞占比 13%。





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 命令注入漏洞(CVE-2020-15778)	101
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	58
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	58
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	58
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	58
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	57
高	OpenSSH 安全漏洞(CVE-2016-1908)	56
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	55
高	OpenSSH 'schnorr.c'远程内存破坏漏洞(CVE-2014-1692)	52
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	41

5、安全漏洞整改情况

5 月网络与信息中心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 1706 种，web 漏洞类型增多 64 种。5 月发放漏洞整改通知书 76 份，完成 4 个信息系统复检，总计 7 次。

对比 4 月，本月高危漏洞类型增加 54 种，高危漏洞个数增加 589 个，总的漏洞类型增加 61 种，总的漏洞数量增加 59 个。

网络与信息中心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。