中国地质大学（武汉）网络安全月报

2021 年 06 月　（第 W0064 期）　总第 64 期

中国地质大学（武汉）网络与信息中心　2021 年 06 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 1176974 起，其中服务器受到攻击的事件共计 653441 起；网站受到攻击的事件共计 578823 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。

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

网络安全事件汇总表

序号	时间	内容	处理结果
1	6 月 2 日	教育行业漏洞报告平台通报我校某学院存在信息泄露漏洞问题漏洞	已整改
2	6 月 8 日	教育行业漏洞报告平台通报我校某学院存在暗链漏洞问题	已整改
3	6 月 8 日	教育行业漏洞报告平台通报我校某学院存在暗链漏洞问题	已整改
4	6 月 10 日	教育行业漏洞报告平台通报我校某学院存在敏感信息泄露问题	已整改
5	6 月 16 日	教育行业漏洞报告平台通报我校某学院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 6 月，防火墙防护服务器受到攻击事件共 653441 起；其中针对学校门户站群系统的攻击次数达到 110081 起，占总数的 16.85%。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	110081	16.85%
2	地质科技情报	99282	15.19%
3	教师个人主页发布系统	74432	11.39%
4	地球科学在线	63815	9.77%
5	校园网 VPN 服务	29059	4.45%
6	第二站群系统	20581	3.15%
7	中国地质大学出版社有限责任公司	14282	2.19%
8	湖北省学苑珠宝职业培训学校	12189	1.87%
9	图书馆主页	10906	1.67%
10	检测数据查询	9166	1.40%
11	其他	209648	32.08%
12	所有	653441	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：共发现高危漏洞798种，中危漏洞1393种，低危漏洞308种，漏洞种类较上月明显减少。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。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。

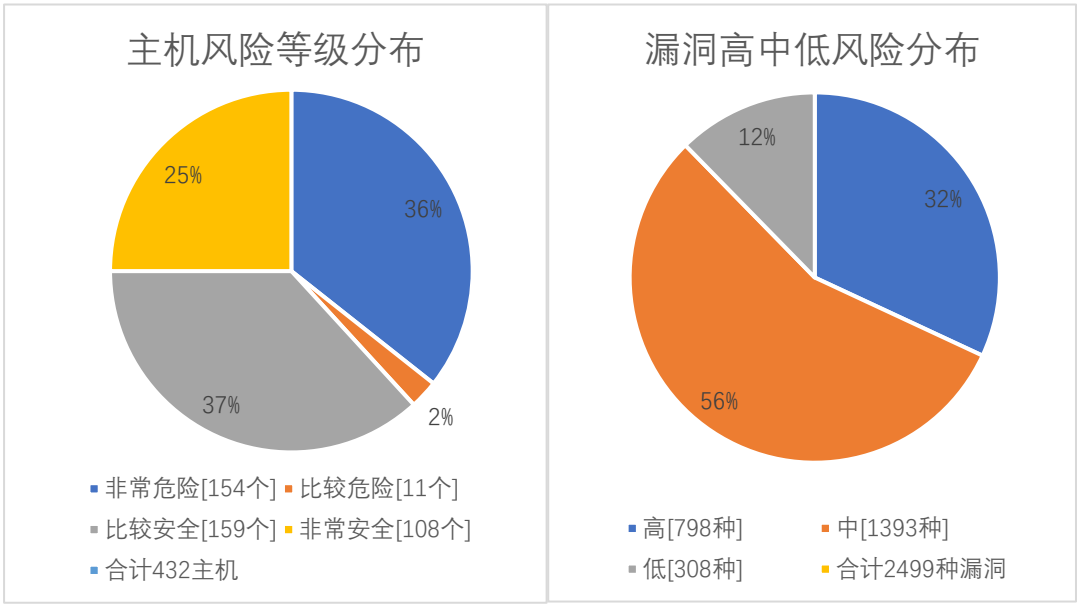
本月漏洞数量较上月明显减少，7月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
5月	2992	4399	2928	10319
6月	3045	4431	2781	10257
变化量（个）	+53	+32	-147	-62

漏洞种类	主机高危	主机中危	主机低危	合计
5月	796	1488	321	2605
6月	798	1393	308	2499
变化量（种）	+2	-95	-13	-106

在本月扫描的432台服务器中，主机漏洞2499种，主机漏洞总计10257个，其中高危漏洞798种，总计3045个；中危漏洞1393种，总计4431个；低危漏洞308，总计2781个。主机风险等级中，非常危险的占36%，比较危险的占2%，比较安全的占37%，非常安全的占25%。漏洞风险等级中，高危漏洞占

比 32%，中危漏洞占比 56%，低危漏洞占比 12%。



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)	153
高	OpenSSH 命令注入漏洞(CVE-2020-15778)	62
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	61
高	CentOS GNU grub2 缓冲区溢出漏洞(CVE-2020-10713)	58
高	CentOS ISC BIND 资源管理错误漏洞(CVE-2020-8616)	51
高	CentOS Bind Server 缓冲区溢出漏洞(CVE-2018-5742)	34
高	CentOS ISC BIND 安全漏洞(CVE-2018-5743)	34
高	CentOS ISC BIND 安全漏洞(CVE-2020-8617)	34
高	CentOS ISC BIND 资源管理错误漏洞(CVE-2019-6477)	34
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	34

5、安全漏洞整改情况

6 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 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 1940 种，web 漏洞类型增多 15 种。5 月发放漏洞整改通知书 56 份，完成 3 个信息系统复检，总计 6 次。

对比 5 月，本月高危漏洞类型增加 2 种，高危漏洞个数增加 53 个，总的漏洞类型减少 106 种，总的漏洞数量减少 62 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。