中国地质大学（武汉）网络安全月报

2021 年 07 月　　（第 W0065 期）　　总第 65 期

中国地质大学（武汉）信息化工作办公室　　2021 年 07 月 31 日

1、情况综述

根据监测分析，7 月份我校校园网络发生的安全威胁事件共计 1353751 起，其中服务器受到攻击的事件共计 712324 起；网站受到攻击的事件共计 641427 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。

7 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

7 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	7 月 6 日	教育行业漏洞报告平台通报我校某信息系统存在信息泄露漏洞问题	已整改
2	7 月 8 日	教育行业漏洞报告平台通报我校某信息系统存在弱口令漏洞问题	已整改
3	7 月 8 日	教育行业漏洞报告平台通报我校某信息系统存在任意文件读取漏洞问题	已整改
4	7 月 12 日	教育行业漏洞报告平台通报我校某信息系统存在任意文件上传漏洞问题	已整改
5	7 月 20 日	教育行业漏洞报告平台通报我校某信息系统存在信息泄露漏洞问题漏洞	已整改

3、服务器受攻击情况

本次监测时间为 7 月，防火墙防护服务器受到攻击事件共 712324 起；其中针对学校门户站群系统的攻击次数达到 128662 起，占总数的 18.06%。门户站群系统提供我校 154 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	128662	18.06%
2	教师个人主页发布系统	109637	15.39%
3	地质科技情报	103126	14.48%
4	地球科学在线	64868	9.11%
5	湖北省学苑珠宝职业培训学校	37613	5.28%
6	校园网 VPN 服务	34767	4.88%
7	第二站群系统	25114	3.53%
8	中国地质大学出版社有限责任公司	17975	2.52%
9	中国地质大学珠宝学院	12384	1.74%
10	检测数据查询	8018	1.13%
11	其他	170160	23.89%
12	所有	712324	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：共发现高危漏洞670种，中危漏洞1184种，低危漏洞273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。

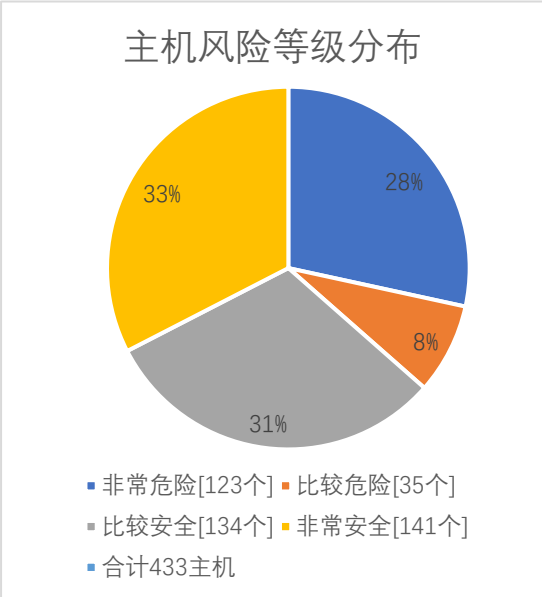
本月漏洞数量较上月明显减少，8月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

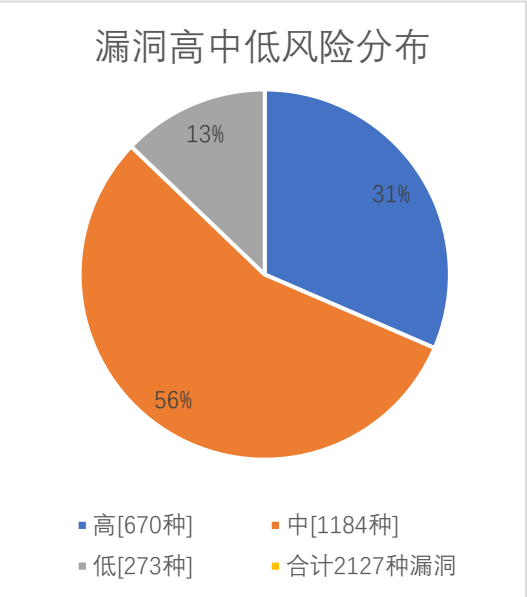
漏洞数量	主机高危	主机中危	主机低危	合计
7月	1877	3136	2400	7413
6月	3045	4431	2781	10257
变化量（个）	-1168	-1295	-381	-2844

漏洞种类	主机高危	主机中危	主机低危	合计
7月	670	1184	273	2127
6月	798	1393	308	2499
变化量（种）	-128	-209	-35	-372

在本月扫描的433台服务器中，主机漏洞2127种，主机漏洞总计7413个，其中高危漏洞670种，总计1877个；中危漏洞1184种，总计3136个；低危漏洞273，总计2400个。主机风险等级中，非常危险的占28%，比较危险的占8%，比较安全的占31%，非常安全的占33%。漏洞风险等级中，高危漏洞占

比 31%，中危漏洞占比 56%，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	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	65
高	nginx 安全漏洞(CVE-2021-23017)	43
高	Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】	25
高	Apache 安全漏洞(CVE-2021-26691)	17
高	Apache 代码问题漏洞(CVE-2021-31618)	17
高	Apache 安全漏洞(CVE-2021-26690)	17
高	Apache HTTP Server 安全漏洞(CVE-2020-35452)	17
高	Apache Tomcat 安全漏洞（CVE-2021-25329）	16
高	CentOS Linux kernel 路径遍历漏洞(CVE-2020-28374)	15
高	CentOS Linux kernel 内存错误引用漏洞(CVE-2021-3347)	15

5、安全漏洞整改情况

7 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 6 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 676 种，web 漏洞类型增多 10 种。7 月发放漏洞整改通知书 53 份，完成 9 个信息系统复检，总计 15 次。

对比 6 月，本月高危漏洞类型减少 128 种，高危漏洞个数减少 1168 个，总的漏洞类型减少 372 种，总的漏洞数量减少 2844 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。