中国地质大学（武汉）网络安全月报

2021 年 12 月　　（第 W0070 期）　　总第 70 期

中国地质大学（武汉）信息化工作办公室　　2021 年 12 月 31 日

1、情况综述

根据监测分析，12 月份我校校园网络发生的安全威胁事件共计 1289934 起，其中服务器受到攻击的事件共计 698776 起；网站受到攻击的事件共计 591158 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。

12 月份我校总体网络安全情况良好，处理网络安全事件共 4 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

12 月处理网络安全事件共 8 起。其中湖北省等保通报办公室通报事件 2 起，教育系统网络安全工作管理平台通报事件 1 起，喻家山派出所通报事件 1 起，关山街道办事处通报事件 1 起，其他通报事件 3 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	12 月 9 号	湖北省等保通报办公室通报我校某信息系统存在弱口令问题	已整改
2	12 月 16 号	赛尔网络通报我校疑似存在挖矿行为	已整改
3	12 月 20 号	关山街道办事处通报我校疑似存在挖矿行为	已整改
4	12 月 22 日	喻家山派出所通报我校某系统存在信息泄露问题	已整改
5	12 月 23 号	赛尔网络通报某信息系统存在外链问题	已整改
6	12 月 23 号	赛尔网络通报某信息系统存在外链问题	已整改
7	12 月 30 号	教育系统网络安全工作管理平台通报我校某信息系统存在暗链问题	已整改

8	12 月 30 号	湖北省等保通报办公室通报我校某信息系统存在命令执行问题	已整改

3、服务器受攻击情况

本次监测时间为 12 月，防火墙防护服务器受到攻击事件共 698776 起；其中针对学校门户站群系统的攻击次数达到 101338 起，占总数的 14.40%。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	189326	27.09%
2	第一站群系统	101338	14.50%
3	地球科学在线	58539	8.38%
4	校园网 VPN 服务	26432	3.78%
5	中国地质大学出版社有限责任公司	17911	2.56%
6	地质科技情报	17749	2.54%
7	第二站群系统	15559	2.23%
8	中国地质大学珠宝学院	14234	2.04%
9	中国地质大学图书馆-首页	13129	1.88%
10	检测数据查询	11832	1.69%
11	其他	232727	33.30%
12	所有	698776	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：共发现高危漏洞588 种，中危漏洞 1111 种，低危漏洞 282 种，漏洞种类较上月明显增多。

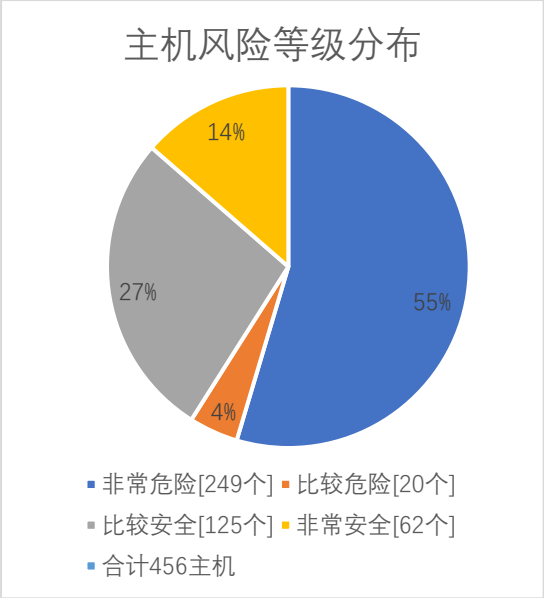
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

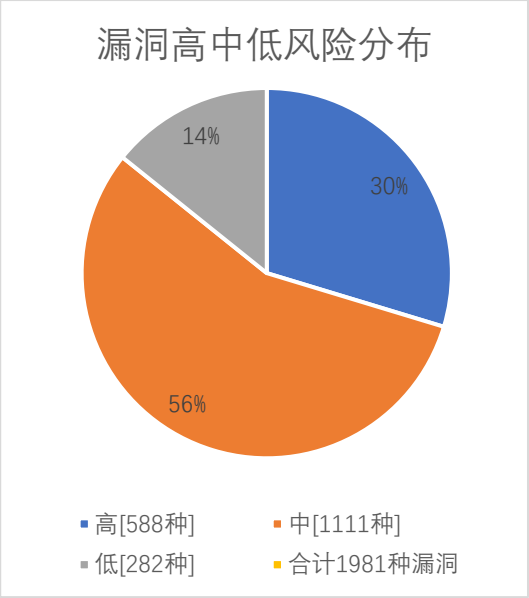
本月漏洞数量较上月明显增多，1 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
12 月	2571	3604	3279	9454
11 月	2414	2852	3138	8404
变化量（个）	+157	+752	+141	+1050

漏洞种类	主机高危	主机中危	主机低危	合计
12 月	588	1111	282	1981
11 月	553	937	274	1726
变化量（种）	+35	+174	+8	+255

在本月扫描的 456 台服务器中，主机漏洞 1981 种，主机漏洞总计 9454 个，其中高危漏洞 588 种，总计 2571 个；中危漏洞 1111 种，总计 3604 个；低危漏洞 282 种，总计 3279 个。主机风险等级中，非常危险的占 55%，比较危险的占 4%，比较安全的占 27%，非常安全的占 14%。漏洞风险等级中，高危漏洞占比 30%，中危漏洞占比 56%，低危漏洞占比 14%。





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)	122
高	OpenSSH 安全漏洞(CVE-2021-41617)	101
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	74
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	45
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	44
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	44
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	44
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	44
高	OpenSSH 安全漏洞(CVE-2016-1908)	42
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	42

5、安全漏洞整改情况

12 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 11 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 1279 种，web 漏洞类型增多 10 种。12 月发放漏洞整改通知书 96 份，完成 10 个信息系统复检，总计 10 次。

对比 11 月，本月高危漏洞类型增多 35 种，高危漏洞个数增多 157 个，总的漏洞类型增多 255 种，总的漏洞数量增多 1050 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。