中国地质大学（武汉）网络安全月报

2022 年 1 月　（第 W0071 期）　总第 71 期

中国地质大学（武汉）信息化工作办公室　2022 年 1 月 31 日

1、情况综述

根据监测分析，1 月份我校校园网络发生的安全威胁事件共计 1308401 起，其中服务器受到攻击的事件共计 718496 起；网站受到攻击的事件共计 589905 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 0 个。

1 月份我校总体网络安全情况良好，处理网络安全事件共 14 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

1 月处理网络安全事件共 14 起。其中教育部通报事件 1 起，行业通报事件 10 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	1 月 10 号	教育部通报我校某信息系统存在 sql 注入问题	已整改
2	1 月 12 日	教育行业通报我校某信息系统存在弱口令问题	已整改
3	1 月 12 日	教育行业通报我校某信息系统存在弱口令问题	已整改
4	1 月 12 日	教育行业通报我校某信息系统存在弱口令问题	已整改
5	1 月 12 日	教育行业通报我校某信息系统存在 sql 注入问题	已整改
6	1 月 12 日	教育行业通报我校某信息系统存在敏感信息泄漏问题	已整改
7	1 月 12 日	教育行业通报我校某信息系统存在文件上传问题	已整改
8	1 月 19 日	教育行业通报我校某信息系统存在弱口令问题	已整改

9	1 月 19 日	教育行业通报我校某信息系统存在弱口令问题	已整改
10	1 月 19 日	教育行业通报我校某信息系统存在敏感信息泄漏问题	已整改
11	1 月 19 日	赛尔网络安全服务团队发现我校某信息系统存在非法外链问题	已整改
12	1 月 19 日	赛尔网络安全服务团队发现我校某信息系统存在非法外链问题	已整改
13	1 月 19 日	赛尔网络安全服务团队发现我校某信息系统存在非法外链问题	已整改

3、服务器受攻击情况

本次监测时间为 1 月，防火墙防护服务器受到攻击事件共 718496 起；其中针对学校门户站群系统的攻击次数达到 98891 起，占总数的 13.76%。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	187174	26.05%
2	第一站群系统	98891	13.76%
3	校园网 VPN 服务	45983	6.40%
4	地球科学在线	45697	6.36%
5	第二站群系统	17551	2.44%
6	中国地质大学珠宝学院	14695	2.05%
7	中国地质大学图书馆-首页	14368	2.00%
8	地质科技情报	14092	1.96%
9	中国地质大学出版社有限责任公司	13459	1.87%
10	检测数据查询	11452	1.59%
11	其他	255134	35.51%
12	所有	718496	100.00%

4、服务器漏洞扫描分析

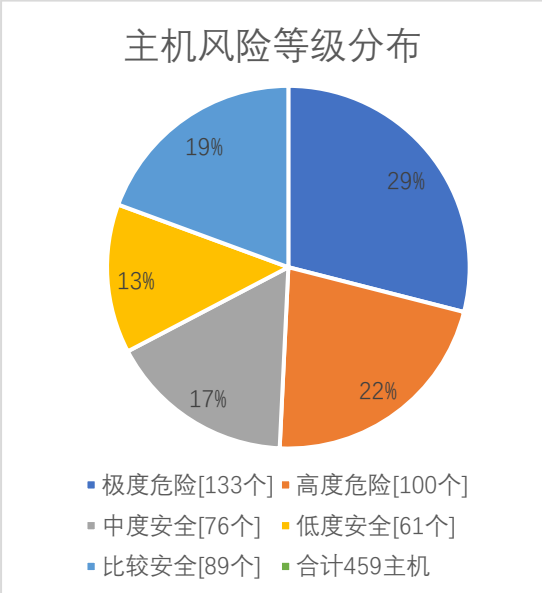
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1169 个，中危漏洞 4477 个，低危漏洞 3694 个，漏洞数量较上月明显增多。

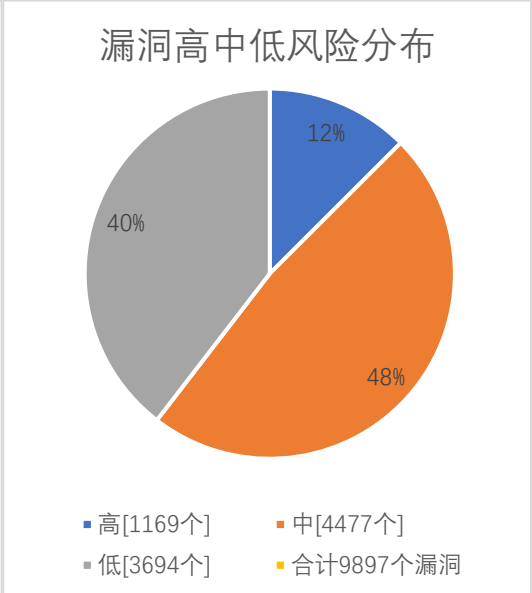
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

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
1 月	1169	4477	3694	9897
变化量（个）	-1402	+873	+415	+443

在本月扫描的 459 台服务器中，主机漏洞总计 9897 个，其中高危漏洞 1169 个；中危漏洞 4477 个；低危漏洞 3694 个。主机风险等级中，极度危险的占 29%，高度危险的占 22%，中度危险的占 17%，低度危险的占 13%，比较安全占 19%。漏洞风险等级中，高危漏洞占比 12%，中危漏洞占比 48%，低危漏洞占比 40%。





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)	38
高	OpenSSH'ssh/kex.c'拒绝服务漏洞(CVE-2016-8858)	38
高	OpenSSH 安全漏洞(CVE-2016-10009)	38
高	OpenSSH sshd 安全漏洞(CVE-2016-6515)	38
高	OpenSSH 安全漏洞(CVE-2016-10012)	38
高	OpenSSH 安全漏洞(CVE-2016-1908)	35
高	OpenSSH sshd 权限许可和访问控制漏洞 CVE-2015-5600	35
高	OpenSSH‘hash_buffer’函数缓冲区溢出漏洞(CVE-2014-1692)	32
高	OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478)	20
高	Microsoft Windows SMB 输入验证漏洞(CVE-2017-0144)(方程式工具-永恒之蓝)[原理扫描]	13

5、安全漏洞整改情况

1 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 12 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 282 种，web 漏洞类型增多 7 种。1 月发放漏洞整改通知书 117 份，完成 8 个信息系统复检，总计 18 次。

对比 12 月，本月高危漏洞个数减少 1402 个，总的漏洞数量增多 443 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。