中国地质大学（武汉）网络安全月报

2021 年 09 月　　（第 W0067 期）　总第 67 期

中国地质大学（武汉）信息化工作办公室　　2021 年 09 月 30 日

1、情况综述

根据监测分析，9 月份我校校园网络发生的安全威胁事件共计 1323748 起，其中服务器受到攻击的事件共计 706090 起；网站受到攻击的事件共计 617658 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。

9 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

9 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	9 月 2 号	教育行业漏洞报告平台通报我校某信息系统存在代码执行问题	已整改
2	9 月 3 号	教育行业漏洞报告平台通报我校某信息系统存在代码执行问题	已整改
3	9 月 13 号	教育行业漏洞报告平台通报我校某信息系统存在敏感信息泄露问题	已整改
4	9 月 18 号	教育行业漏洞报告平台通报我校某信息系统存在敏感信息泄露问题	已整改
5	9 月 24 号	教育行业漏洞报告平台通报我校某信息系统存在双非网站，弱密码问题	已整改

3、服务器受攻击情况

本次监测时间为 9 月，防火墙防护服务器受到攻击事件共 706090 起；其中针对学校门户站群系统的攻击次数达到 172828 起，占总数的 24.48%。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	172828	24.48%
2	教师个人主页发布系统	94394	13.37%
3	地球科学在线	55423	7.85%
4	校园网 VPN 服务	41298	5.85%
5	第二站群系统	38052	5.39%
6	中国地质大学出版社有限责任公司	17865	2.53%
7	地质科技情报	16028	2.27%
8	中国地质大学珠宝学院	15217	2.16%
9	中国地质大学图书馆	14259	2.02%
10	检测数据查询	10309	1.46%
11	其他	230417	32.63%
12	所有	706090	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：共发现高危漏洞504种，中危漏洞941种，低危漏洞267种，漏洞种类较上月明显减少。

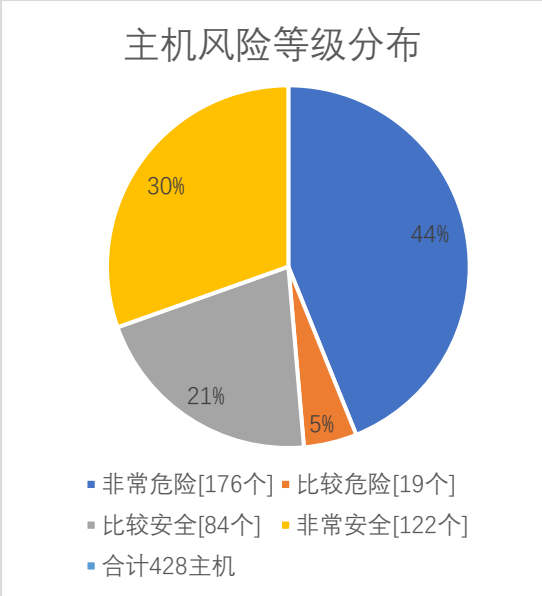
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报信息化工作办公室进行复检。

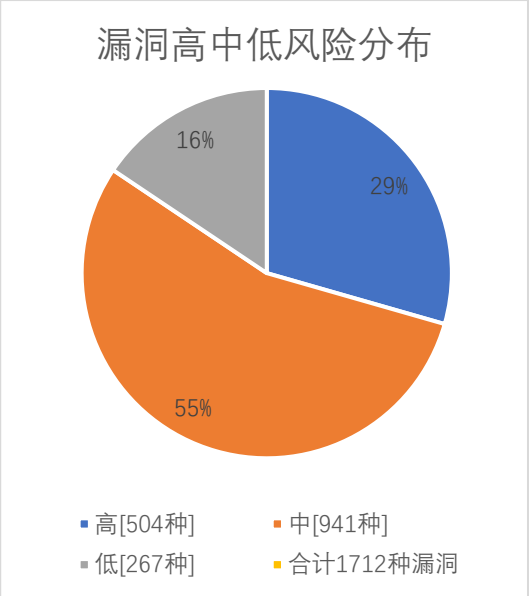
本月漏洞数量较上月明显减少，10月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报信息化工作办公室进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
9月	1594	2314	2341	6249
8月	2500	4000	3090	9590
变化量（个）	-906	-1686	-749	-3341

漏洞种类	主机高危	主机中危	主机低危	合计
9月	504	941	267	1712
8月	799	1396	309	2504
变化量（种）	-295	-455	-42	-792

在本月扫描的401台服务器中，主机漏洞1712种，主机漏洞总计6249个，其中高危漏洞504种，总计1594个；中危漏洞941种，总计2314个；低危漏洞267，总计2341个。主机风险等级中，非常危险的占44%，比较危险的占5%，比较安全的占21%，非常安全的占30%。漏洞风险等级中，高危漏洞占比29%，中危漏洞占比55%，低危漏洞占比16%。





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)	76
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	60
高	nginx 安全漏洞(CVE-2021-23017)	37
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	34
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	34
高	OpenSSH 'schnorr.c'远程内存破坏漏洞(CVE-2014-1692)	34
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	34
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	34
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	34
高	OpenSSH 安全漏洞(CVE-2016-1908)	32

5、安全漏洞整改情况

9 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 8 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 171 种，web 漏洞类型增多 1 种。9 月发放漏洞整改通知书 41 份，完成 5 个信息系统复检，总计 5 次。

对比 8 月，本月高危漏洞类型减少 295 种，高危漏洞个数减少 906 个，总的漏洞类型减少 792 种，总的漏洞数量减少 3341 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。