中国地质大学（武汉）网络安全月报

2020 年 08 月　　（第 W0054 期）　　总第 54 期

中国地质大学（武汉）网络与信息中心　　2020 年 08 月 31 日

1、情况综述

根据监测分析，8 月份我校校园网络发生的安全威胁事件共计 3739724 起，其中服务器受到攻击的事件共计 3433318 起；网站受到攻击的事件共计 306406 起；可能感染病毒木马的僵尸主机共 18 台，其中确定的僵尸主机共 4 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

8 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

8 月处理网络安全事件共 5 起。其中教育系统通报安全事件 4 起，湖北省教育厅通报 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	8 月 19 日	接上级部门通报学校某系统存在越权查看他人信息漏洞	已整改
2	8 月 19 日	接上级部门通报学校某学院存在敏感信息泄露问题	已整改
3	8 月 19 日	接上级部门通报学校某单位存在弱密码和逻辑漏洞	已整改
4	8 月 27 日	接上级部门通报学校某网站出现涉黄信息	已整改 s
5	8 月 29 日	接上级部门通报学校某教师收到钓鱼邮件	已整改

3、服务器受攻击情况

本次监测时间为 8 月，防火墙防护服务器受到攻击事件共 3433318 起；其中针对学校门户站群系统的攻击次数达到 442711 起，占总数的 12.9%。门户站群系统提供我校 144 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	站群系统（旧版）	442711	12.9%
2	第一站群系统	64488	1.9%
3	第二战群系统	37881	1.1%
4	校园网 VPN 服务	20363	0.6%
5	地质科技情报	19491	0.6%
6	地球科学在线	12417	0.4%
7	图书馆主页	11102	0.3%
8	中国地质大学出版社有限责任公司（含中国地质大学出版社职教分社）	9181	0.3%
9	远程教学管理平台	7745	0.2%
10	研究生管理信息系统	7090	0.2%
11	其他	2800849	81.6%
12	所有	3433318	100%

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：共发现高危漏洞555种，中危漏洞1973种，低危漏洞428种，漏洞种类较上月明显减少。

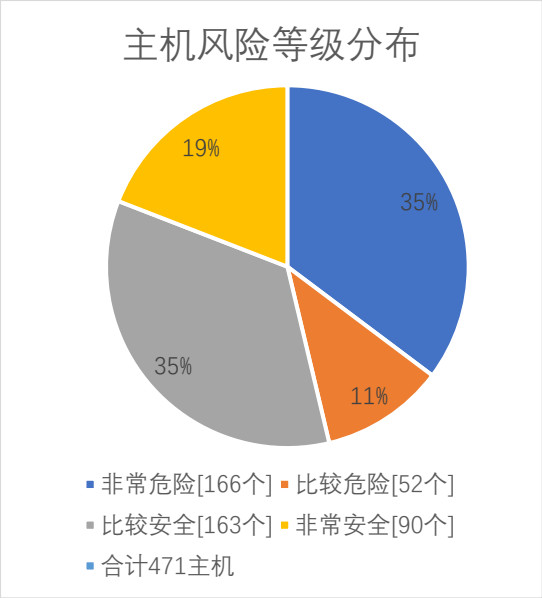
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络与信息中心将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络与信息中心进行复检。

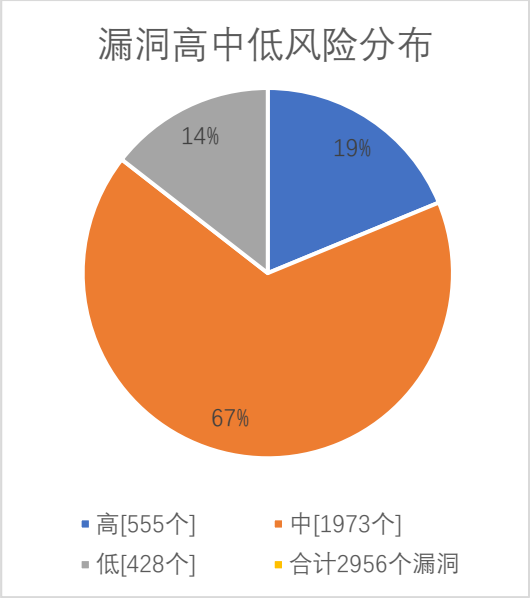
本月漏洞数量较上月明显减少，9月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
7月份	3124	11064	4607	18795
8月份	2588	9527	4803	16918
变化量（个）	-536	-1537	-136	-1841

漏洞种类	主机高危	主机中危	主机低危	合计
7月份	557	2027	429	3013
8月份	555	1973	428	2956
变化量（种）	-2	-54	-1	-57

在本月扫描的471台服务器中，主机漏洞共计2956种，主机漏洞总计16918个。其中高危漏洞555种，总计2588个；中危漏洞1973种，总计9527个；低危漏洞428种，总计4803个。主机风险等级中，非常危险的占35%，比较危险的占11%，比较安全的占35%，非常安全的占19%。漏洞风险等级中，高危漏洞占比19%，中危漏洞占比67%，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 MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	62
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	63
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	63
高	OpenSSH 安全漏洞(CVE-2016-1908)	62
高	OpenSSH ’schnorr.c’远程内存破坏漏洞(CVE-2014-1692)	60
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	60
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	62
高	Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】	24
高	OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478)	27

高	Apache HTTP Server mod_ssl 空指针间接引用漏洞(CVE-2017-3169)	16

5、安全漏洞整改情况

8 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 7 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 2230 种，web 漏洞类型增多 12 种。8 月发放漏洞整改通知书 88 份，完成 11 个信息系统复检，总计复检 16 次。

对比 7 月，本月高危漏洞类型减少 2 种，高危漏洞个数减少 536 个，总的漏洞类型减少 57 种，总的漏洞数量减少 1841 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。