中国地质大学（武汉）网络安全月报

2020 年 06 月　（第 W0052 期）　总第 52 期

中国地质大学（武汉）网络与信息中心　2020 年 06 月 30 日

1、情况综述

根据监测分析，6 月份我校校园网络发生的安全威胁事件共计 2784341 起，其中服务器受到攻击的事件共计 2478517 起；网站受到攻击的事件共计 305824 起；可能感染病毒木马的僵尸主机共 15 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。

6 月份我校总体网络安全情况良好，处理网络安全事件共 3 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

6月处理网络安全事件共3起。其中教育系统通报安全事件2起，预警通报 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	6 月 3 日	接上级部门通报学校某学院网站存在敏感信息泄露	已删除
2	6 月 8 日	接上级部门通报学校某单位移动应用存在后门-app 安全威胁	已处理
3	6 月 24 日	关于启明星辰运维安全网关存在高危漏洞的预警通报	已处理

3、服务器受攻击情况

本次监测时间为 6 月，防火墙防护服务器受到攻击事件共2479062 起;其中针对学校门户站群系统的攻击次数达到 415124 起，占总数的 16.7%。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	415124	16.7%
2	中国地质大学校园虚拟专用网络（VPN）服务	37927	1.5%
3	地球科学在线	27899	1.1%
4	第二套站群系统	17341	0.7%
5	地质科技情报	13502	0.5%
6	研究生管理信息系统	11067	0.4%
7	图书馆主页	9269	0.4%
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)	8890	0.4%
9	检测数据查询	6690	0.3%
10	校外访问平台	8459	0.7%
11	其他	1925006	77.7%
12	所有	2479062	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 500 种，中危漏洞 1904 种，低危漏洞 417 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。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。

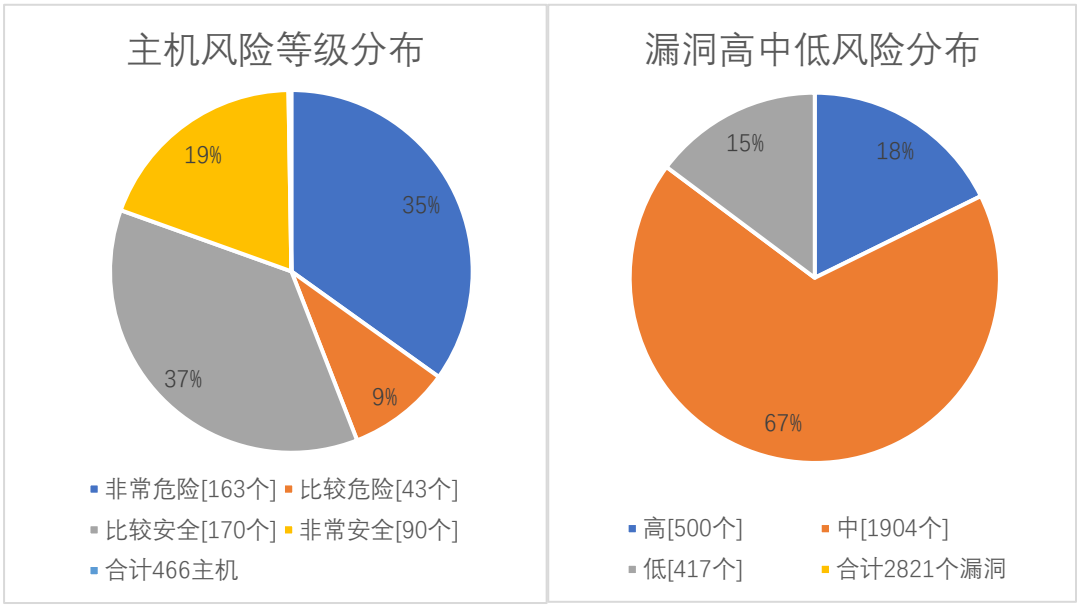
本月漏洞数量较上月明显增多，6 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
5 月份	2766	9679	4928	17373
6 月份	3193	10516	4743	18452
变化量（个）	+427	+837	-185	+1079

漏洞种类	主机高危	主机中危	主机低危	合计
5 月份	503	1883	419	2805
6 月份	500	1904	417	2821
变化量（种）	-3	+21	-2	+16

在本月扫描的 466 台服务器中，主机漏洞共计 2821 种，主机漏洞总计 18452 个。其中高危漏洞 500 种，总计 3193 个；中危漏洞 1904 种，总计 10516 个；低危漏洞 417 种，总计 4743 个。主机风险等级

中，非常危险的占 35%，比较危险的占 9%，比较安全的占 37%，非常安全的占 19%。漏洞风险等级中，高危漏洞占比 18%，中危漏洞占比 67%，低危漏洞占比 15%。



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 远程代码执行漏洞(CVE-2016-10009)	67
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	67
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	66
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	66
高	OpenSSH 安全漏洞(CVE-2016-1908)	66
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	66
高	OpenSSH ’schnorr.c’远程内存破坏漏洞(CVE-2014-1692)	64
高	OpenSSH J-PAKE 授权问题漏洞(CVE-2010-4478)	28
高	Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】	22

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

6 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 5 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 7585 种，web 漏洞类型增多 19 种。根据数据分析，由于 8 台主机的上线，导致高危漏洞数量增加。6 月发放漏洞整改通知书 49 份，完成 15 个信息系统复检，总计 29 次。

对比 5 月，本月高危漏洞类型减少 3 种，高危漏洞个数增加 427 个，总的漏洞类型增加 16 种，总的漏洞数量增加 1079 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。