中国地质大学（武汉）网络安全月报

2020 年 10 月　（第 W0056 期）　总第 56 期

中国地质大学（武汉）网络与信息中心　2020 年 10 月 31 日

1、情况综述

根据监测分析,10 月份我校校园网络发生的安全威胁事件共计 4421493 起，其中服务器受到攻击的事件共计 4002752 起；网站受到攻击的事件共计 418741 起;可能感染病毒木马的僵尸主机共 9 台，其中确定的僵尸主机共 13 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

10 月份我校总体网络安全情况良好，处理网络安全事件共 6 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

10 月处理网络安全事件共 6 起。其中教育系统通报安全事件 4 起，网络舆情事件 2 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	10 月 5 日	教育行业漏洞报告平台某系统存在文件上传导致 XSS 漏洞问题。	已整改
2	10 月 6 日	教育行业漏洞报告平台某系统 SQL 注入问题。	已整改
3	10 月 18 日	教育行业漏洞报告平台某系统存在敏感信息泄露问题。	已整改
4	10 月 27 日	教育网通报某机房电脑存在访问恶意 IP 问题。	已整改
5	10 月 28 日	协助处置微博舆情事件。	已处置
6	10 月 31 日	协助处置舆情事件。	已处置

3、服务器受攻击情况

本次监测时间为 10 月，防火墙防护服务器受到攻击事件共 4002752 起；其中针对学校门户站群系统的攻击次数达到 1325512 起，占总数的 33.1%。门户站群系统提供我校 154 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	1325512	33.1%
2	教师个人主页发布系统	380776	9.5%
3	第二站群系统	76694	1.9%
4	地球科学在线	44402	1.1%
5	图书馆主页	18772	0.5%
6	校园网 VPN 服务	16822	0.4%
7	地质科技情报	14553	0.4%
8	检测数据查询	8942	0.2%
9	统一身份权限管理系统	7155	0.2%
10	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）	6934	0.2%
11	其他	2102190	52.2%
12	所有	4002752	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：共发现高危漏洞655种，中危漏洞1777种，低危漏洞377种，漏洞种类较上月明显增多。

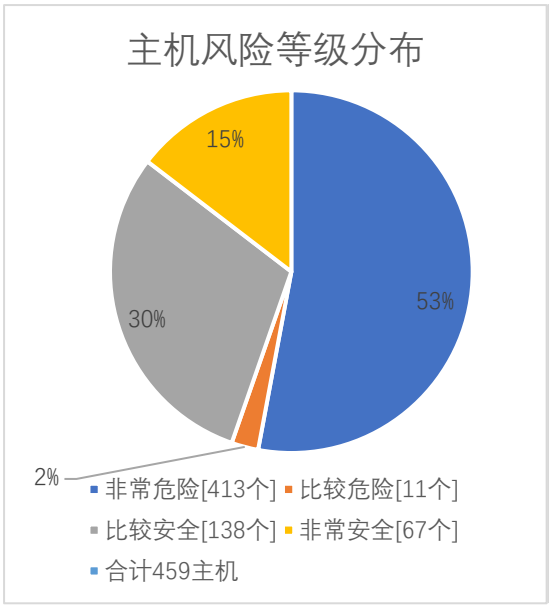
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络与信息中心将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络与信息中心进行复检。

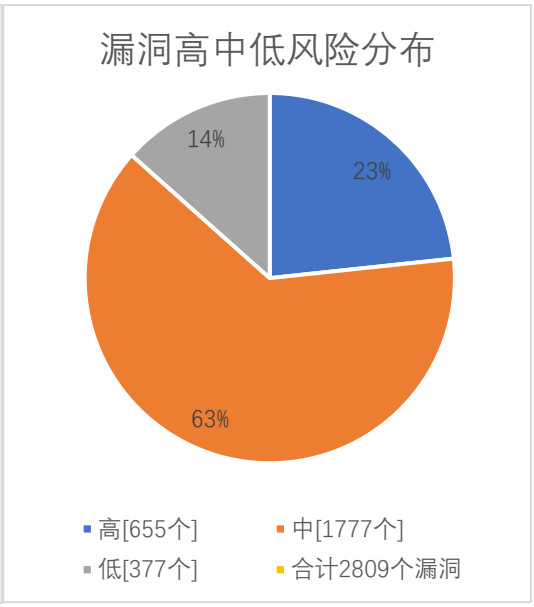
本月漏洞数量较上月明显减少，10月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
9月份	2459	9037	4386	15882
10月份	3439	7475	3954	14868
变化量（个）	+980	-1562	-432	-1014

漏洞种类	主机高危	主机中危	主机低危	合计
9月份	460	1437	366	2263
10月份	655	1777	377	2809
变化量（种）	+195	+340	+11	+546

在本月扫描的459台服务器中，主机漏洞共计2809种，主机漏洞总计14868个。其中高危漏洞655种，总计3439个；中危漏洞1777种，总计7475个；低危漏洞377种，总计3954个。主机风险等级中，非常危险的占53%，比较危险的占2%，比较安全的占30%，非常安全的占15%。漏洞风险等级中，高危漏洞占比23%，中危漏洞占比63%，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)	137
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	66
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	66
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	65
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	66
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	65
高	OpenSSH 安全漏洞(CVE-2016-1908)	64
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	64
高	OpenSSH ’schnorr.c’远程内存破坏漏洞(CVE-2014-1692)	61
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	38

5、安全漏洞整改情况

10 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 9 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 7109 种，web 漏洞类型增多 4 种。10 月发放漏洞整改通知书 120 份，完成 4 个信息系统复检，总计 7 次。

对比 9 月，本月高危漏洞类型增加 195 种，高危漏洞个数增加 980 个，总的漏洞类型增加 546 种，总的漏洞数量减少 1014 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。