中国地质大学（武汉）网络安全月报

2020 年 05 月　（第 W0051 期）　总第 51 期

中国地质大学（武汉）网络与信息中心　2020 年 05 月 31 日

1、情况综述

根据监测分析，5 月份我校校园网络发生的安全威胁事件共计 1561896 起，其中服务器受到攻击的事件共计 1275482 起；网站受到攻击的事件共计 286414 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 2 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 2 个。

5 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

5 月处理网络安全事件共 6 起。其中教育系统网络安全工作管理平台通报事件 2 起，安全预警通知公告 3 起，校园舆情事件 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	5 月 9 日	某学院网站存在未授权访问	已整改
2	5 月 13 日	某学院网站存在未授权访问	已整改
3	5 月 25 日	关于深信服 SSL VPN 设备存在高危漏洞的预警通告	已接收
4	5 月 25 日	关于防范网络攻击的预警通告	已发布
5	5 月 25 日	协助处理校园舆情事件 1 起	已删除
6	5 月 28 日	关于 SaltStack 软件存在高危漏洞的预警通告	已发布

3、服务器受攻击情况

本次监测时间为 5 月，防火墙防护服务器受到攻击事件共1275482 起;其中针对学校门户站群系统的攻击次数达到 396300 起，占总数的 31.1%。门户站群系统提供我校 143 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	396300	31.1%
2	地球科学在线	24534	1.9%
3	校园网 VPN	21325	1.7%
4	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)	12383	1%
5	图书馆主页	9322	0.7%
6	研究生管理信息系统	8689	0.7%
7	校外访问平台	8459	0.7%
8	检测数据查询	6048	0.5%
9	教师个人主页发布系统	5756	0.5%
10	地质科技情报	4343	0.3%
11	其他	778323	61%
12	所有	1275482	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 503 种，中危漏洞 1883 种，低危漏洞 419 种，漏洞种类较上月持平。

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。

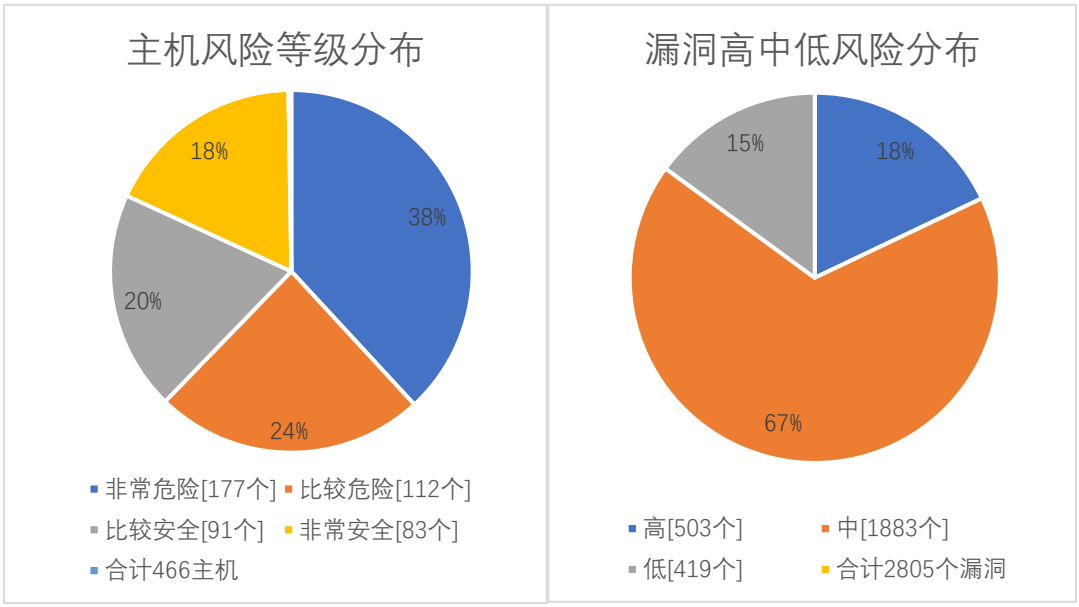
本月漏洞数量较上月明显增多，6 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
4 月份	2694	9579	4908	17181
5 月份	2766	9679	4928	17373
变化量（个）	+72	+100	+20	+192

漏洞种类	主机高危	主机中危	主机低危	合计
4 月份	489	1843	426	2758
5 月份	503	1883	419	2805
变化量（种）	+14	+40	-7	+47

在本月扫描的 466 台服务器中，主机漏洞共计 2805 种，主机漏洞总计 17373 个。其中高危漏洞 503 种，总计 2766 个；中危漏洞 1883 种，总计 9679 个；低危漏洞 419 种，总计 4928 个。主机风险等级中，

非常危险的占 38%，比较危险的占 24%，比较安全的占 20%，非常安全的占 18%。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%。



5、安全漏洞整改情况

5 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 4 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 2500 种，web 漏洞类型增多 11 种。根据数据分析，由于有主机漏洞增多，导致高危漏洞数量增多。

对比 4 月，本月高危漏洞类型增加 20 种，高危漏洞个数增加 82 个，总的漏洞类型增加 47 种，总的漏洞数量增加 192 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。