中国地质大学（武汉）网络安全月报

2020 年 01 月　　（第 W0047 期）　总第 47 期

中国地质大学（武汉）网络与信息中心　　2020 年 01 月 31 日

1、情况综述

根据监测分析，1 月份我校总体网络安全情况良好，处理网络安全事件共 1 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

1 月处理网络安全事件共 1 起。本月共教育行业漏洞报告平台通报事件 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	1 月 12 日	教育行业漏洞报告平台通报我校某学院信息管理系统存在弱口令问题	已修复

3、服务器受攻击情况

本次监测时间为1月,防火墙防护服务器受到攻击事件共564718起；其中针对学校门户站群系统的攻击次数达到220023起，占总数的39%。门户站群系统提供我校137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	220023	39%
2	地质科技情报	16868	3%
3	地球科学在线	12364	2.20%
4	日志审计系统	7418	1.30%
5	检测数据查询	6872	1.20%
6	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）	6643	1.20%
7	远程教学管理平台	5292	0.90%
8	教师个人主页发布系统	4948	0.90%
9	图书馆主页	4522	0.80%
10	中国地质大学校园虚拟专用网络服务	3871	0.70%
11	其他	275897	48.90%
12	所有	564718	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 455 种，中危漏洞 1689 种，低危漏洞 411 种，漏洞种类较上月基本持平。

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。

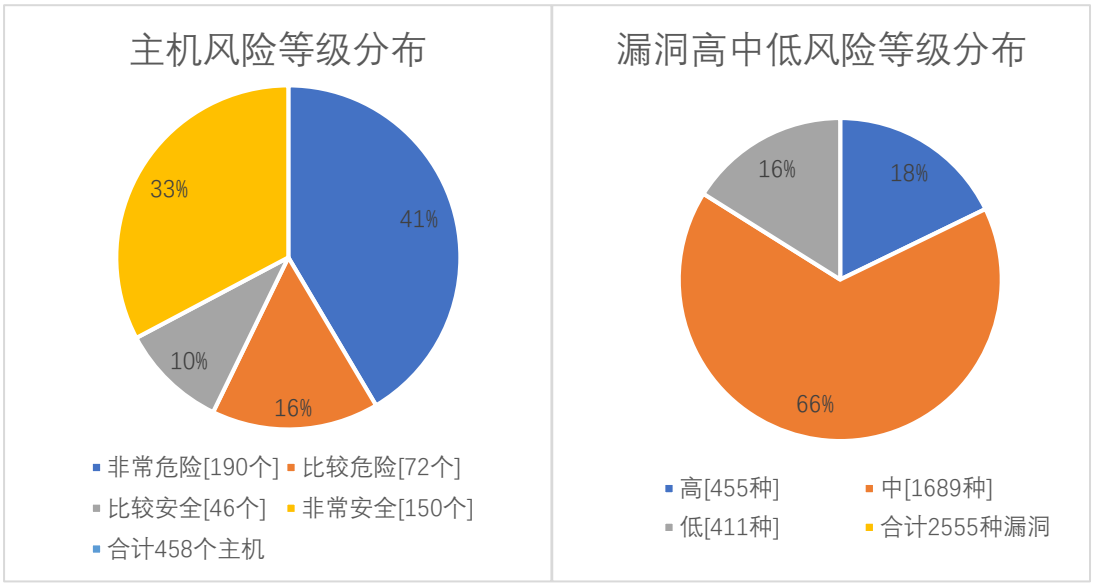
本月漏洞数量较上月明显增加，2 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
12 月份	2317	7214	4660	14191
1 月份	2995	10063	5134	18192
变化量（个）	+678	+2849	+474	+4001

漏洞种类	主机高危	主机中危	主机低危	合计
12 月份	452	1689	440	2581
1 月份	455	1689	411	2555
变化量（种）	+3	0	-29	-26

在本月扫描的 458 台服务器中，主机漏洞共计 2555 种，主机漏洞总计 18192 个。其中高危漏洞 455 种，总计 2995 个；中危漏洞 1689

种，总计 10063 个；低危漏洞 411 种，总计 5134 个。主机风险等级中，非常危险的占 41%，比较危险的占 16%，比较安全的占 10%，非常安全的占 33%。漏洞风险等级中，高危漏洞占比 16%，中危漏洞占比 66%，低危漏洞占比 18%。



5、安全漏洞整改情况

1 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 12 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 25371 种，应用漏洞类型无变化。根据数据分析，由于六台主机的上线，导致高危漏洞数量增加。对比 12 月，本月高危漏洞类型增加 3 种，高危漏洞个数增加 678 个，总的漏洞数量增加 4001 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。