中国地质大学（武汉）网络安全月报

2021 年 01 月　　（第 W0059 期）　　总第 59 期

中国地质大学（武汉）网络与信息中心　　2021 年 02 月 01 日

1、情况综述

根据监测分析，1 月份我校校园网络发生的安全威胁事件共计 3756205 起，其中服务器受到攻击的事件共计 3297344 起；网站受到攻击的事件共计 458861 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 10 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 2 个。

1 月份我校总体网络安全情况良好，处理网络安全事件共 0 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 0 起。

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 3297344 起；其中针对学校门户站群系统的攻击次数达到 168108 起，占总数的 5.10%。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	168108	5.10%
2	校园网 VPN 服务	52693	1.60%
3	教师个人主页发布系统	39790	1.21%
4	地球科学在线	25256	0.77%
5	第二站群系统	22001	0.67%
6	数字校园门户	21463	0.65%
7	地质科技情报	11572	0.35%
8	图书馆主页	10623	0.32%
9	检测数据查询	7463	0.23%
10	校外访问平台	6721	0.20%
11	其他	2931654	88.91%

12	所有	3297344	100.00%

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：共发现高危漏洞1156种，中危漏洞1754种，低危漏洞353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。

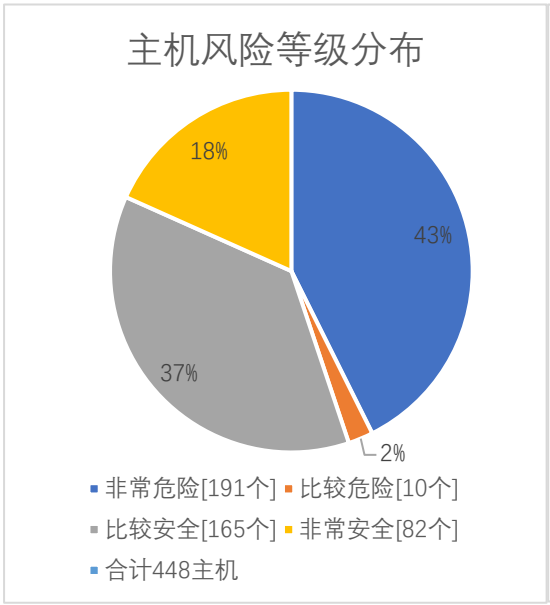
本月漏洞数量较上月明显减少，2月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

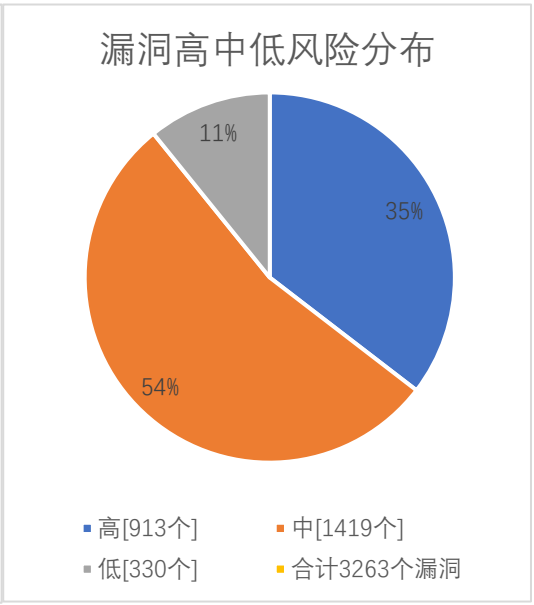
漏洞数量	主机高危	主机中危	主机低危	合计
12月份	3668	5100	3694	12462
1月份	4386	6263	3438	14087
变化量（个）	+718	+1163	-256	+1625

漏洞种类	主机高危	主机中危	主机低危	合计
12月份	913	1419	330	2662
1月份	1156	1754	353	3263
变化量（种）	+243	+335	+23	+601

在本月扫描的448台服务器中，主机漏洞共计3263种，主机漏洞总计14087个。其中高危漏洞1156种，总计4386个；中危漏洞1754种，总计6263个；低危漏洞353种，总计3438个。主机风险等级中，非常危险的占43%，比较危险的占2%，比较安全的占37%，非常安全的占18%。漏洞风险等级中，高危漏

洞占比 35%，中危漏洞占比 54%，低危漏洞占比 11%。





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)	90
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	52
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	52
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	52
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	52
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	52
高	OpenSSH 安全漏洞(CVE-2016-1908)	51
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	51
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	39
高	OpenSSH 'schnorr.c'远程内存破坏漏洞(CVE-2014-1692)	48

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 2095 种，web 漏洞类型增多 9 种，8 月发放漏洞整改通知书 93 份，完成 11 个信息系统复检，总计 49 次。

对比 12 月，本月高危漏洞类型增多 243 种，高危漏洞个数增多 718 个，总的漏洞类型增多 601 种，总的漏洞数量增多 1625 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。