中国地质大学网络安全月报

2019 年 12 月　　（第 W0046 期）　总第 46 期

中国地质大学（武汉）网络与信息中心　　2019 年 12 月 31 日

1、情况综述

根据监测分析，12 月份我校校园网络发生的安全威胁事件共计 1615223 起，其中服务器受到攻击的事件共计 709262 起；网站受到攻击的事件共计 311476 起；可能感染病毒木马的僵尸主机共 21 台，其中确定的僵尸主机共 4 台；对外发生的 DoS 攻击事件共 0 起，被植入黑链的网站共 0 个。除此之外暂无其他网络安全事件发送,一切正常。

本月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

12 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 12 月，防火墙防护服务器受到攻击事件共 709262 起；其中针对学校门户站群系统的攻击次数达到 392373 起，占总数的 55.3%。门户站群系统提供我校 136 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	目标服务器名称	攻击次数
1	站群发布系统	392373
2	中国地质大学校园虚拟专用网络（VPN）服务	53697
3	地球科学在线	27196
4	教师个人主页发布系统	25340
5	中国地质大学（武汉）研究生管理信息系统	23072
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）	14251
7	远程教学管理平台	7114
8	图书馆主页	6560
9	地质科技情报	4098
10	检测数据查询	3761
11	其他	151800
12	所有	709262

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 452 种，中危漏洞 1689 种，低危漏洞 440 种。

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，整改后上报网络中心进行复检。

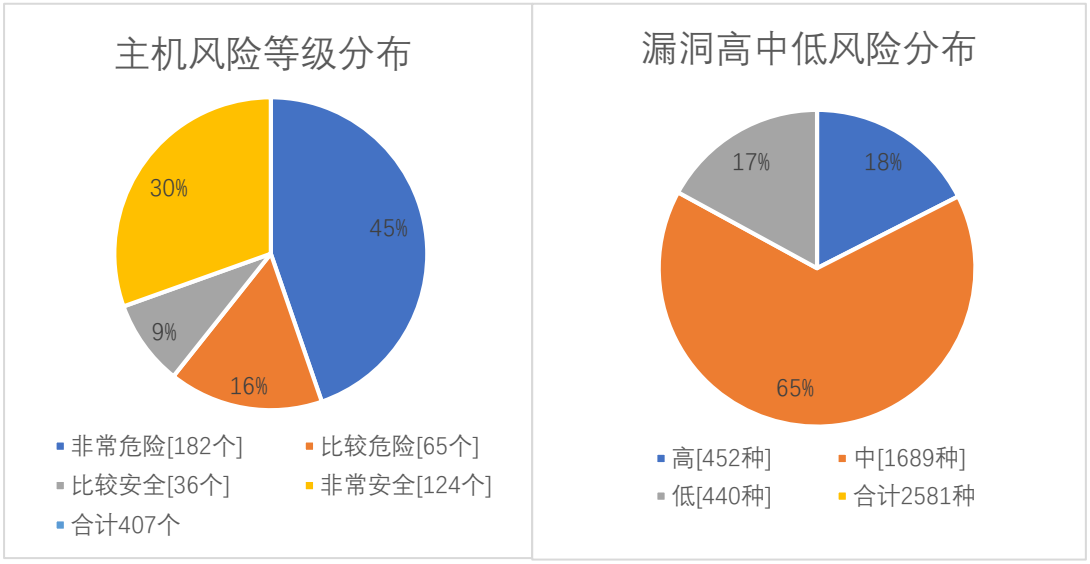
本月漏洞数量较上月基本持平，12 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
11 月份	3276	10530	5607	19413
12 月份	2317	7214	4660	14191
变化量（个）	-959	-3316	+947	-5222

漏洞种类	主机高危	主机中危	主机低危	合计
11 月份	650	1890	442	2982
12 月份	452	1689	440	2581
变化量（种）	-198	-201	-2	-401

在本月扫描的 407 台服务器中，主机漏洞 22581 种，总计 14191 个。其中高危漏洞 452 种，总计 2317 个；中危漏洞 1689 种，总计 7214 个；低危漏洞 440 种，总计 4660 个。主机风险等级中，非常危险的占 45%，比较危险的占 16%，比较安全的占 9%，非常安全的占 30%。

漏洞风险等级中，高危漏洞占比 18%，中危漏洞占比 65%，低危漏洞占比 17%。



5、安全漏洞整改情况

12 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 11 月，漏洞库更新，漏洞类型增多，其中主机漏洞增多 10195 种。经过整改，高危漏洞类型降低 198 种，高危漏洞个数减少 959 个，总的漏洞数量降低 5222 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。