中国地质大学网络安全月报

2019 年 11 月　　（第 W0045 期）（发布）　　总第 45 期

中国地质大学（武汉）网络与信息中心　　2019 年 11 月 30 日

1、情况综述

根据监测分析，11 月份我校校园网络发生的安全威胁事件共计 1701363 起，其中服务器受到攻击的事件共计 548099 起；网站受到攻击的事件共计 221950 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 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

11 月处理网络安全事件共 3 起。其中，教育平台通报事件 2 起，白帽子平台通报事件 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-11-2	“教育行业漏洞报告平台”通报我校一学院存在敏感信息泄露	已修复
2	2019-11-8	“教育系统网络安全工作管理平台” 通报我校一学院存在个人隐私信息泄露	已修复
3	2019-11-15	“教育系统网络安全工作管理平台”通报一学院管理的双非网站存在 SQL 盲注入漏洞。	已修复

3、服务器受攻击情况

本次监测时间为 11 月，防火墙防护服务器受到攻击事件共548099 起；其中针对学校门户站群系统的攻击次数达到 337713 起，占总数的61.6%。门户站群系统提供我校 112 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	337713
2	地球科学在线	122567
3	中国地质大学校园虚拟专用网络	24972
4	图书馆主页	7894
5	中国地质大学珠宝学院-质检网	7808
6	远程与继续教育网站	5433
7	中国地质大学数字校园门户	3105
8	地质科技情报	2741
9	教师个人主页发布系统	2482
10	统一通讯管理平台	2433
11	其他	30951
总计		548099

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：共发现高危漏洞650 种，中危漏洞 1890 种，低危漏洞 442 种。

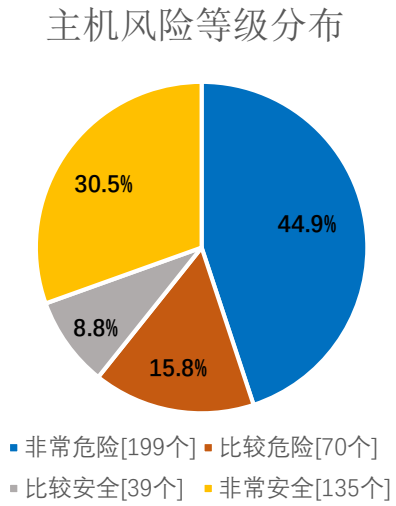
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络中心将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络中心进行复检。

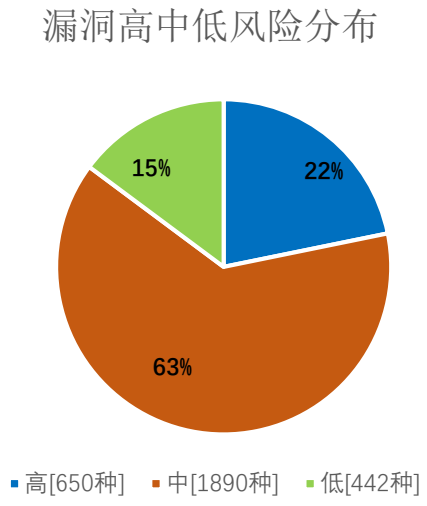
本月漏洞数量较上月基本持平,12月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网信中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
10月份	4210	12681	5437	22328
11月份	3276	10530	5607	19413
变化量（个）	-934	-2151	+134	-2915

漏洞种类	主机高危	主机中危	主机低危	合计
10月份	1355	3024	653	5032
11月份	650	1890	442	2982
变化量（种）	-705	-1134	-221	-2050

在本月扫描的443台服务器中，主机漏洞2982种，总计19413个。其中高危漏洞650种，总计3276个；中危漏洞1892种，总计10530个；低危漏洞442种，总计5607个。主机风险等级中，非常危险的占44.9%，比较危险的占15.8%，比较安全的占8.8%，非常安全的占30.5%。漏洞风险等级中,高危漏洞占比22%,中危漏洞占比63%,低危漏洞占比15%。





5、安全漏洞整改情况

11 月网信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 10 月，漏洞库更新，漏洞类型增多，其中主机漏洞增多 845 种。经过整改，高危漏洞类型降低 705 种，高危漏洞个数减少 934 个，总的漏洞数量降低 2915 个。

网信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。