中国地质大学校园网络安全月报

2018 年 12 月　（第 2018-12 期）　总第 36 期

中国地质大学（武汉）网络与信息中心　2019 年 1 月 10 日

1、情况综述

2018 年 12 月我校总体网络安全情况良好，未发生网络安全事件。

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 992996 起，服务器受到攻击的事件共 413693 起；可能感染病毒木马的僵尸主机共 35 台，其中确定的僵尸主机共 25 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。

2、安全事件通报

12 月未发生网络安全事件。

3、用户终端情况

本月对校园网无线接入用户终端（59.71.224.0-59.71.255.255）进行主动安全扫描。扫描识别到 528 台终端用户设备。发现漏洞 258 个，其中高危漏洞 111 个，严重漏洞 147 个。以 Windows 系统安全漏洞为主，建议用户及时更新 Windows 操作以及相关系统补丁。

危害排名前五的漏洞列表

序号	名称	危害程度	主机数量
1	Microsoft Windows XP 不支持的安装检测	严重	32
2	Microsoft Windows SMBv1 多个漏洞	严重	23
3	MS17-010:Microsoft Windows SMB	严重	22
4	Intel 管理引擎不安全读写操作 RCE (INTEL-SA-00075)	严重	9
5	MS12-020：远程桌面中的漏洞可允许远程代码执行 (2671387)	严重	11

4、服务器受攻击情况

本月服务器受到攻击事件共 413693 起，较 11 月份呈上升趋势。其中针对学校门户站群系统的攻击次数达到 230383 起，占总数的 55.7%。门户站群系统提供我校 121 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

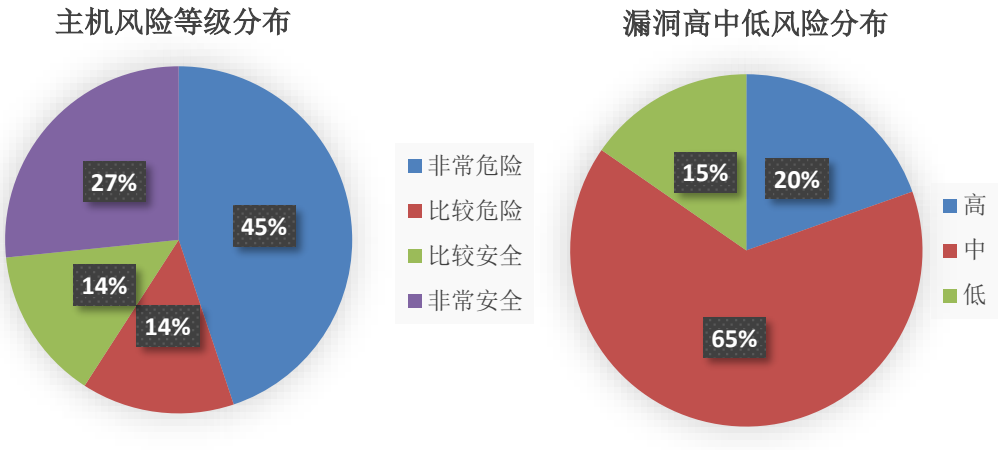
序号	网站	受到攻击次数
1	学校门户站群系统	230383
2	地质科技情报编辑部网站	23005
3	地大期刊社安全与环境工程编辑部采编服务系统	14438
4	地球科学期刊服务器	12801
5	网络中心微信服务器	11819
6	校办服务器	9942
7	后勤服务器	8589
8	外语实验中心服务器	8487
9	网络中心反向代理服务器	8001
10	校办正方系统	6608
其他		79620
总计		**413693**

5、服务器漏洞扫描分析

12 月 20 日，对校园网服务器进行漏洞扫描。结果统计如下：共发现高危漏洞 504 个，中危漏洞 1674 个，低危漏洞 395 个。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。本月扫描结果高危漏洞数量有所增加，1 月将采取防火墙策略收缩措施，限制部分存在严重高危漏洞的服务器访问权限，督促接收单位尽快如期完成漏洞整改工作，并上报网络中心进行复检。

在扫描的近 500 台服务器中，主机风险等级中，非常危险的占 44.9%，比较危险的占 14.3%，比较安全的占 14.3%，非常安全的占 26.6%。漏洞风险等级中，高危漏洞占比 19.6%，中危漏洞占比 65.1%，低危漏洞占比 15.4%。



6、安全漏洞整改情况

网络与信息中心对扫描出来的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。截止 12 月 31 日，已累计下发系统整改报告共计 327 份，其中 216 个系统整改完毕，通过复测。其中，本月下发系统整改报告共计 110 份，其中 85 个系统整改完毕，通过复测。

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，全校应在管理和意识方面对网络安全引起足够重视。