中国地质大学网络安全月报

2018 年 11 月　（第 W0035 期）（发布）　总第 35 期

中国地质大学（武汉）网络与信息中心　2018 年 12 月 10 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 1096573 起，服务器受到攻击的事件共 379948 起;可能感染病毒木马的僵尸主机共 54 台，其中确定的僵尸主机共 30 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。

本月我校总体网络安全情况良好，处理网络安全事件共？起，未发生重大的网络安全事件。

2、安全事件通报

11 月处理网络安全事件共 5 起。全部为教育行业安全平台通报。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2018-11-06	一平台未授权访问漏洞	已修复
2	2018-11-14	一网站读取文件安全漏洞	通知负责人处理
3	2018-11-24	一网站弱密码漏洞	通知负责人处理
4	2018-11-27	一网站弱密码漏洞	通知负责人处理
5	2018-11-27	一系统短信发送漏洞	通知负责人处理

3、用户终端情况

本月对校园网无线接入用户终端（172.31.0.0/16）进行主动安全扫描。扫描识别 2957 台终端用户设备。发现漏洞 317 个，其中高

危漏洞 180 个，严重漏洞 137 个。以 Windows 系统安全漏洞为主，建议用户及时更新 Windows 操作以及补丁。

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 SMBv1 多个漏洞	严重	34
2	MS17-010:Microsoft Windows SMB	严重	33
3	Microsoft Windows XP 不支持的安装检测	严重	7
4	Microsoft SQL Server 不受支持的版本检测	严重	6
5	Web Server Directory Traversal Arbitrary File Access	严重	4

4、服务器受攻击情况

本月服务器受到攻击事件共 379948 起，较 10 月份呈略微上升趋势。其中针对学校门户站群系统的攻击次数达到 208612 起，占总数的 54.9%。门户站群系统提供我校 117 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	主机地址	受到攻击次数
1	门户站群系统	208612
2	远程与继续教育学院官网	34446
3	《安全与环境工程》稿件采编平台	18803
4	地球科学在线	7881
5	远程教学管理平台	6843
6	外国语学院官网	6416
7	网络中心反向代理服务器	5937
8	二级单位服务器	4242
9	学工就业服务器	4223
10	地质科技情报	4176
	其他	78369

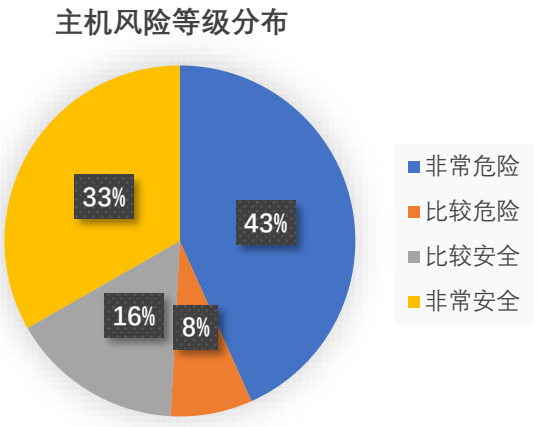
总计	379948

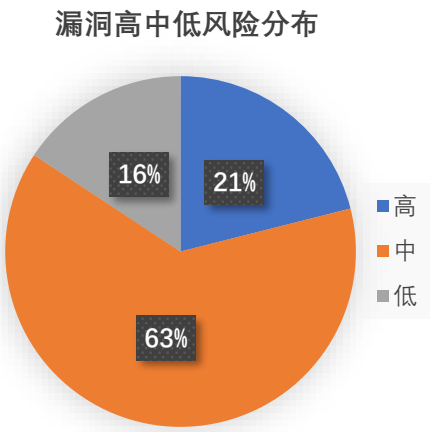
5、服务器漏洞扫描分析

11 月 28 日，对校园网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 490 个，中危漏洞 1471 个，低危漏洞 366 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，12 月将加大整改力度，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 43.3%,比较危险的占 7.5%,比较安全的占 15.9%,非常安全的占 33.3%。漏洞风险等级中，高危漏洞占比 21.1%，中危漏洞占比 63.2%，低危漏洞占比 15.7%。





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 11 月 31 日，已累计下发系统整改报

告共计 223 份，其中 88 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 37 份， 29 个系统整改完毕。

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。