中国地质大学校园网络安全月报

2018 年 10 月　（第 2018-10 期）　总第 34 期

中国地质大学（武汉）网络与信息中心　　2018 年 11 月 10 日

1、情况综述

2018 年 10 月 1 日至 2018 年 10 月 31 日，我校总体网络安全情况良好，未发生重大的网络安全事件。

根据监测分析，10 月份我校校园网络发生的安全威胁事件共 437487 起，服务器受到攻击的事件共 387764 起；可能感染病毒木马的僵尸主机共 44 台，其中确定的僵尸主机共 32 台；对外发生的 DoS 攻击事件共 1 起，被植入黑链的网站共 1 个。

2、安全事件通报

10 月处理网络安全事件共 2 起。其中，教育部通报 1 起，运营商通报 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2018-10-17	一学院珠宝检测网站安全漏洞	已通知负责人修复
2	2018-10-23	一网站 mysql 弱密码安全漏洞	已关停

3、用户终端情况

本月对校园网无线接入用户终端（172.30.0.0/16）进行主动安全扫描。扫描识别 1025 台终端用户设备，发现漏洞 125 个，其中高危漏洞 65 个，严重漏洞 60 个。以 Windows、手机、平板操作系统安全漏洞为主，建议用户及时更新系统补丁。

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 Vista 检测漏洞	严重	21
2	Microsoft Windows SMBv1 多个漏洞	严重	11
3	Microsoft Windows XP 检测漏洞	严重	6
4	MS17-010:Microsoft Windows SMB	严重	5
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 387764 起，较 9 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 192985 起，占总数的 49.8%。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

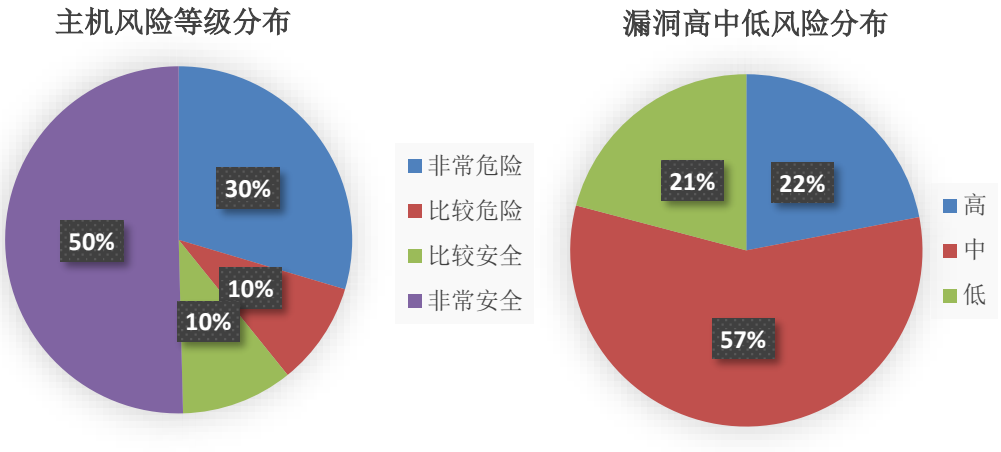
序号	网站	受到攻击次数
1	学校门户站群系统	192985
2	地大期刊社安全与环境工程编辑部采编服务系统	23101
3	计算机学院主页	13955
4	图书馆主页	11182
5	地球科学期刊服务器	8706
6	地质科技情报编辑部网站	8039
7	外语实验中心服务器	7665
8	二级单位主页服务器	6997
9	网院教学平台数据库	6282
10	反向代理服务器	5824
总计		**284736**

5、服务器漏洞扫描分析

10 月 24 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 163 个，中危漏洞 424 个，低危漏洞 155 个。本月扫描结果高危漏洞数量显著下降，主要与 9-10 月大力推进安全漏洞整改工作以及厂商及时发布安全漏洞补丁有关。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。

在扫描的近 500 台服务器中，主机风险等级中，非常危险的占 30%，比较危险的占 10%，比较安全的占 10%，非常安全的占 50%。高风险漏洞占 22%。



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 10 月 31 日，已累计下发系统整改报告共计 181 份，其中 59 个系统整改完毕，通过复测。其中，10 月下发系统整改报告共计 24 份， 16 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，学校应在管理和意识方面对网络安全引起足够重视。