中国地质大学校园网网络安全情况月报

2018 年 9 月　　（第 W0033 期）　 总第 33 期

中国地质大学（武汉）网络与信息中心

1　情况综述

2018 年 9 月 1 日至 2018 年 9 月 30 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。

9 月份，网络与信息中心对服务器所在的 8 个 C 类地址段进行了全方位的漏洞扫描。根据监测分析，我校校园网络发生的安全威胁事件共 496251 起，服务器受到攻击的事件共 233225 起;可能感染病毒木马的僵尸主机共 46 台，其中确定的僵尸主机共 31 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

9 月收到并处理网络安全事件通报 8 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2018-9-3	一网站存在垂直越权安全漏洞	已修复
2	2018-9-15	一平台未授权访问安全漏洞	已修复
3	2018-9-19	非法域名恶意指向安全隐患	已修复
4	2018-9-14	协助处理突发事件	已完成
5	2018-9-20	一平台未授权访问安全漏洞	已修复
6	2018-9-26	协助处理突发事件	已完成
7	2018-9-27	一平台未授权访问安全漏洞	已修复
8	2018-9-27	某学院私接线路影响校园网稳定	已处理

3 用户终端情况

本月对校园网无线接入用户终端（172.29.0.0/16）进行主动安全扫描。扫描识别 2810 台终端用户设备。发现漏洞 177 个，其中高危漏洞 70 个，严重漏洞 107 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 SMBv1 多个漏洞	严重	37
2	MS17-010:Microsoft Windows SMB	严重	29
3	不受支持的 Windows OS	严重	5
4	Web Server Directory Traversal Arbitrary File Access	严重	3
5	PHP 已不受支持的版本检测	严重	3

4 服务器受攻击情况

本月服务器受到攻击事件共 233225 起，较 8 月份呈下降趋势。其中针对学校门户站群系统的攻击次数达到 143223 起，占总数的 61.4%。门户站群系统提供我校 111 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	备注
1	学校门户站群系统	143223	
2	远教学院主页	7838	
3	地球科学期刊主页	6649	
4	计算机学院主页	6080	
5	二级单位主页服务	6061	
6	图书馆主页	5026	
7	网页反向代理服务器	4024	
8	图书馆查新检索服务器	3403	

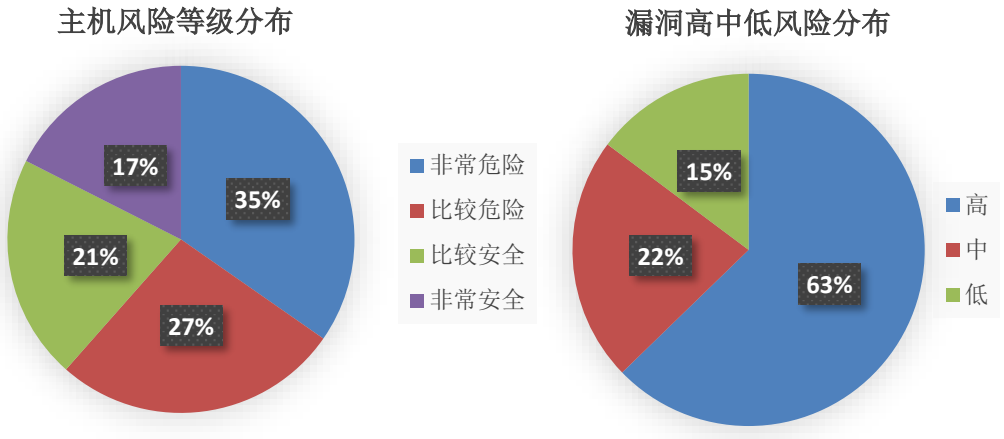
9	出版社主页	3040	
10	招标办主页	2783	
11	其他	45098	
总计		**233225**	

5 服务器漏洞扫描分析

本月对校园网服务器所在的8个C类地址网段进行漏洞扫描结果统计如下：共发现高危漏洞 416 个，中危漏洞 149 个，低危漏洞 98 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。

在扫描的近 500 台服务器中，主机风险等级中，非常危险的占 35%，比较危险的占 27%，比较安全的占 17%，非常安全的仅占 21%。高风险漏洞占 63%。



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。其中 109 个业务系统，13 个系统整改完毕，93 个系统正在整改中，3 个系统因业务调整关闭。

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，网络安全在管理和意识方面应引起全校足够重视。

2018 年 9 月 10 日