中国地质大学网络安全月报

2019 年 05 月　　（第 W0041 期）（发布）　　总第 41 期

中国地质大学（武汉）网络与信息中心　　2019 年 5 月 30 日

1、情况综述

根据监测分析，5 月份我校校园网络发生的安全威胁事件共计 1316128 起，其中服务器受到攻击的事件共计 717381 起；可能感染病毒木马的僵尸主机共 34 台，其中确定的僵尸主机共 26 台；对外发生的 DoS 攻击事件共 1 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 5 起，未发生重大的网络安全事件。

2、安全事件通报

5 月处理网络安全事件共 5 起。其中，教育部通报 2 起、Google 安全告警 1 起、网络安全预警 1 起、校内安全维稳 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-5-5	Google 安全告警	已修复
2	2019-5-5	一学院主页逻辑漏洞	已关停
3	2019-5-16	教育部发布 windows 漏洞预警	已转发
4	2018-5-18	校内舆情事件	已完成
5	2018-5-29	一单位主页权限漏洞	已修复

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。扫描识别到 1311 台终端用户设备。发现漏洞 20 个，其中高危漏洞 11 个，严重漏洞 9 个。其中存在 3 台 windows 主机开放了 RDP 服务，含有 CVE-2019-0708 漏洞，建议尽快处理。

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 RDP RCE (CVE-2019-0708)	严重	3
2	Portable SDK for UPnP Devices (libupnp) < 1.6.18 多种基于堆栈的缓冲区溢出	严重	3
3	X11 Server Unauthenticated Access	严重	2
4	Web Server Directory Traversal Arbitrary File Access	严重	1
5	PHP 7.1.x < 7.1.25 Arbitrary Command Injection Vulnerability	高危	1

4、服务器受攻击情况

本次监测时间为 5 月，服务器受到攻击事件共 717381 起；其中针对学校门户站群系统的攻击次数达到 448633 起，占总数的 62.5%。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	业务名称	受到攻击次数
1	学校门户站群系统	448633
2	地球科学期刊服务器	16651
3	研究生就业网	13846
4	计算机学院主页	13092
5	图书馆	12252
6	教师个人主页	11029
7	地质科技情报网	10736

8	中国地质大学(武汉)秭归产学研基地网站	9935
9	中国地质大学出版社有限责任公司	8683
10	采购与投标管理中心主页	6822
11	其他	165702
总计		**717381**

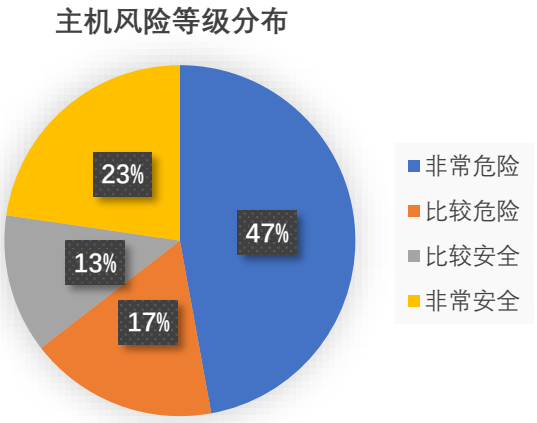
5、服务器漏洞扫描分析

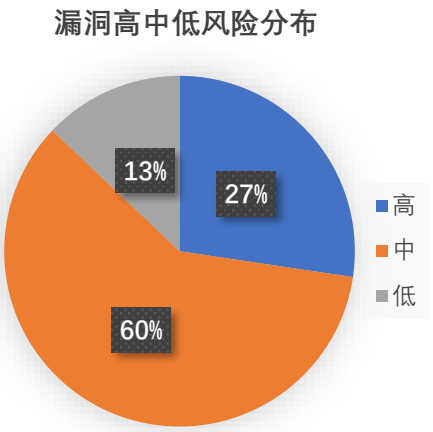
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1336 个，中危漏洞 2917 个，低危漏洞 630 个。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。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有所增加，5 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，并上报网络中心进行复检，保证正常工作用网安全。

在扫描的 454 台服务器中，主机风险等级中，非常危险的占 47.1%，比较危险的占 17.4%，比较安全的占 12.8%，非常安全的占 22.7%。漏洞风险等级中，高危漏洞占比 27.4%，中危漏洞占比 59.7%，低危漏洞占比 12.9%。





6、安全漏洞整改情况

6 月网信中心将加快推进学校信息系统登记备案工作。落实信息系统责任单位，关停未备案信息系统。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。

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。