中国地质大学网络安全月报

2019 年 06 月　　（第 W0042 期）（发布）　　总第 42 期

中国地质大学（武汉）网络与信息中心　　2019 年 6 月 30 日

1、情况综述

根据监测分析，6 月份我校校园网络发生的安全威胁事件共计 1191460 起，其中服务器受到攻击的事件共计 641796 起；可能感染病毒木马的僵尸主机共 32 台，其中确定的僵尸主机共 26 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 2 起，未发生重大的网络安全事件。

2、安全事件通报

6 月处理网络安全事件共 2 起。其中，教育部安全预警 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	2019-6-3	关于 Absolute 公司防盗追踪软件安全风险的提示	已发布
2	2019-6-27	赛尔网络通报两学院网站存在安全漏洞	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 3533 台终端用户设备。发现漏洞 76 个，其中高危漏洞 52 个，严重漏洞 24 个。以 Windows 系统安全漏洞和 Web 应用漏洞为主，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	Web Server Directory Traversal Arbitrary File Access	严重	8
2	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)	严重	4
3	PHP 已不受官方支持的版本检测	严重	4
4	已不受支持的 OpenSSL	严重	2
5	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 多个漏洞	高危	7

4、服务器受攻击情况

本次监测时间为 6 月，服务器受到攻击事件共 641796 起；其中针对学校门户站群系统的攻击次数达到 403271 起，占总数的 62.8%。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	业务名称	受到攻击次数
1	学校门户站群系统	403271
2	地质科技情报网	24349
3	秭归产学研基地网站	20359
4	地球科学期刊服务器	16073
5	研究生就业网	12725
6	网院服务器	11909
7	教师个人主页	9244

8	中国地质大学出版社有限责任公司	7049
9	中国地质大学固体矿产勘查实验教学中心	6356
10	研究生信息管理系统	6331
11	124130	165702
总计		**641796**

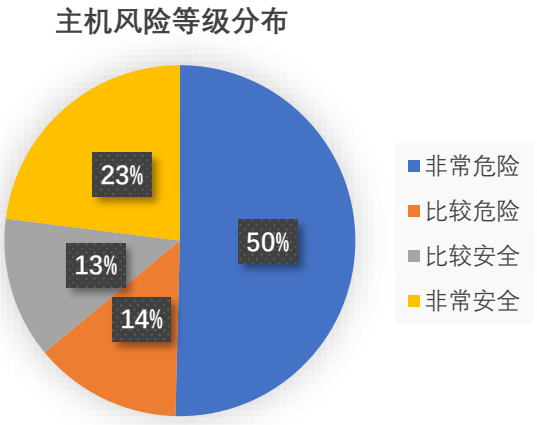
5、服务器漏洞扫描分析

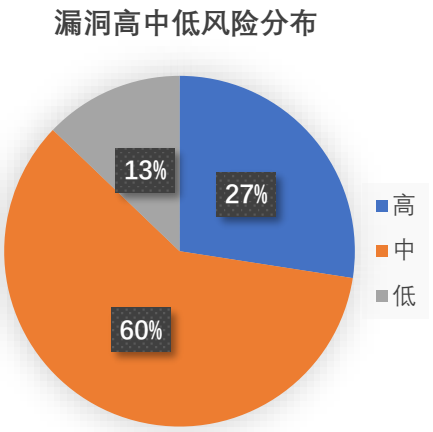
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1362 个，中危漏洞 2962 个，低危漏洞 637 个。

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基本持平，6 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 500 台服务器中，主机风险等级中，非常危险的占 50.4%，比较危险的占 13.6%，比较安全的占 13.0%，非常安全的占 23.0%。漏洞风险等级中，高危漏洞占比 27.5%，中危漏洞占比 59.7%，低危漏洞占比 12.8%。





6、安全漏洞整改情况

6 月网信中心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。