中国地质大学网络安全月报

2019 年 04 月　　（第 W0040 期）（内部）　总第 40 期

中国地质大学（武汉）网络与信息中心　　2019 年 4 月 30 日

1、情况综述

根据监测分析，4 月份我校校园网络发生的安全威胁事件共计 1093979 起，其中服务器受到攻击的事件共计 573728 起；可能感染病毒木马的僵尸主机共 36 台，其中确定的僵尸主机共 27 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 5 起，未发生重大的网络安全事件。

2、安全事件通报

4 月处理网络安全事件共 5 起。其中，教育行业安全平台通报 2 起、运营商通报 2 起、安全预警 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-4-1	一学院网站逻辑漏洞	已关停
2	2019-4-9	一单位网站域名未备案	已修复
3	2019-4-15	一系统安全漏洞	已关停
4	2019-4-18	家属区用户用网不规范	已整改
5	2019-4-25	weblogic 反序列化安全漏洞预警	已发布

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。扫描识别到 3085 台终端用户设备。发现漏洞 34 个，其中高危漏洞 27 个，严重漏洞 7 个。以 Web 应用漏洞为主，建议用户及时

升级 Web 应用版本补丁。

危害排名前五的漏洞列表

序号	名称	危害程度	主机数量
1	PHP 已不受官方支持的版本检测	严重	2
2	Web Server Directory Traversal Arbitrary File Access	严重	1
3	NFS Exported Share Information Disclosure	严重	1
4	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 多个漏洞	高危	4
5	AApache 2.2.x < 2.2.28 多种漏洞	高危	2

4、服务器受攻击情况

本次监测时间为 4 月，服务器受到攻击事件共 573728 起；其中针对学校门户站群系统的攻击次数达到 374111 起，占总数的 65.8%。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	主机地址	受到攻击次数
1	学校门户站群系统	377645
2	图书馆主页	16500
3	地球科学期刊服务器	15256
4	研究生就业网	12422
5	教师个人主页	12414
6	地质科技情报编辑部网站	11871
7	计算机学院主页	9528
8	出版社主页	8692
9	远教学院微信报名系统	8416
10	秭归产学研基地网站	7500
11	其他	93484
总计		**573728**

5、服务器漏洞扫描分析

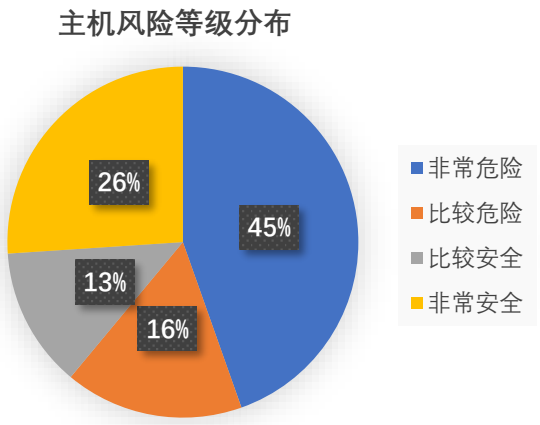
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1347 个，中危漏洞 2969 个，低危漏洞 645 个。

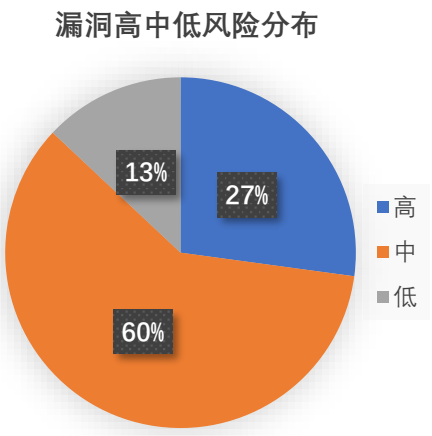
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络中心将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络中心进行复检。

本月针对“WebLogic wls9-async 反序列化远程命令执行漏洞(CNVD-C-2019-488)”进行对使用 WebLogic 的资产进行检查，未发现此类漏洞，就此安全事件已发送相应的预警报告及预防措施。

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 480 台服务器中，主机风险等级中，非常危险的占 45%，比较危险的占 16%，比较安全的占 13%，非常安全的占 26%。漏洞风险等级中，高危漏洞占比 27%，中危漏洞占比 60%，低危漏洞占比 13%。





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 4 月 30 日， 共计 214 台服务器存在高危漏洞风险，待学校信息系统（网站）整理汇总工作完成后，统一下发整改报告。

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。