中国地质大学校园网络安全月报

2019 年 3 月　　（第 2019-02 期）　总第 38 期

中国地质大学（武汉）网络与信息中心　　2019 年 4 月 10 日

1、情况综述

3 月我校总体网络安全情况良好，处理网络安全事件共 7 起，未发生重大的网络安全事件。

根据监测分析，3 月我校校园网络发生的安全威胁事件共计 1123157 起，其中服务器受到攻击的事件共计 570303 起；可能感染病毒木马的僵尸主机共 33 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。

2、安全事件通报

3 月处理网络安全事件共 7 起。其中，教育行业安全平台通报 3 起、运营商通报 1 起、校内安全维稳 2 起、教育部网络威胁预警 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-3-8	协助排查一系统安全隐患	已完成
2	2019-3-11	处理恶意域名指向	已修复
3	2019-3-16	发布防范勒索病毒预警	已完成
4	2019-3-18	协助处理舆情问题	已完成
5	2019-3-20	一学院主页安全漏洞	已修复
6	2019-3-20	一系统安全漏洞	已修复
7	2019-3-21	一学院主页安全漏洞	已修复

3、用户终端情况

3 月对校园网无线接入用户终端（172.31.0.0-172.31.255.255）进行主动安全扫描。扫描识别到 3113 台终端用户设备。发现漏洞 74 个，其中高危漏洞 49 个，严重漏洞 25 个。以 Windows 系统安全漏洞和 Web 应用漏洞为主，建议用户及时更新 Windows 操作系统以及相关 Web 应用补丁。

危害排名前五的漏洞列表

序号	名称	危害程度	主机数量
1	Web Server Directory Traversal Arbitrary File Access	严重	10
2	MS15-034：HTTP.sys 中的漏洞可允许远程代码执行	严重	6
3	PHP 已不受官方支持的版本检测	严重	2
4	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 多个漏洞	高危	3
5	Oracle TNS Listener Remote Poisoning	高危	2

4、服务器受攻击情况

3 月检测到服务器受攻击事件共 570303 起；其中针对学校门户站群系统的攻击次数达到 378275 起，占总数的 66.3%。门户站群系统提供我校 124 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	378275
2	地大期刊社安全与环境工程编辑部采编服务系统	19216
3	地球科学期刊服务器	15825
4	旧版二级单位主页服务器	15097
5	图书馆主页	11009
6	地质科技情报编辑部网站	10312
7	计算机学院主页	9992
8	反向代理服务器	9158
9	网院教学平台、数据库	8803
10	外语实验中心服务器	8785
其他		83831
总计		**570303**

5、服务器漏洞扫描分析

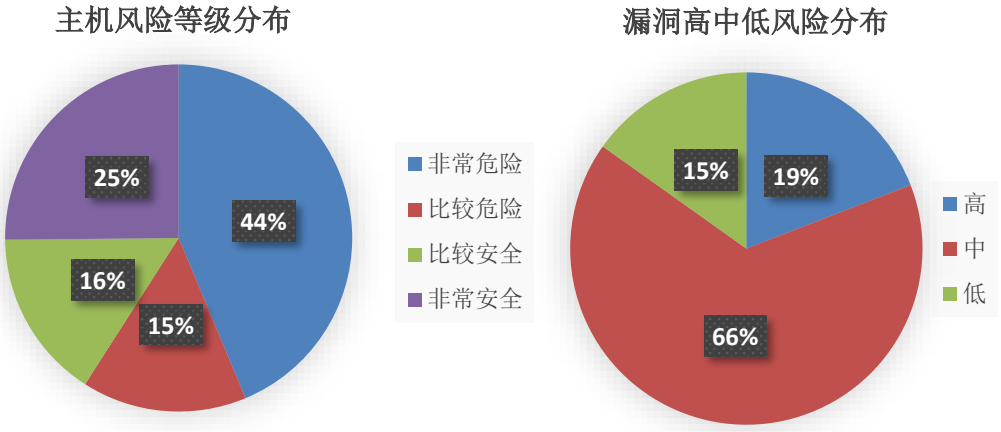
3 月对校园数据中心进行漏洞扫描检测，共发现高危漏洞 530 个，中危漏洞 1820 个，低危漏洞 420 个。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络与信息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，整改后上报网络与信息中心进行复检。

3 月漏洞数量较上月明显减少，4 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，并上报网络与信息中心进行复检，保证正常工作用网安全。

在扫描的 475 台服务器中，主机风险等级中，非常危险的占 43.7%，比较危险的占 15.4%，比较安全的占 15.8%，非常安全的占 25.2%。漏洞风险等级中，高危漏洞占比 19.1%，中危漏洞占比 65.7%，低危漏洞占比 15.2%。



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。截至 3 月 29 日，281 个系统整改完毕，通过复测，6 个系统关停，剩余 188 个存在高危漏洞风险的系统正在整改。

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，并通知到所属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，全校应在管理和意识方面对网络安全引起足够重视。