中国地质大学网络安全月报

2019 年 10 月　　（第 W0044 期）（发布）　　总第 44 期

中国地质大学（武汉）网络与信息中心　　2019 年 10 月 30 日

1、情况综述

根据监测分析，10 月份我校校园网络发生的安全威胁事件共计 1712962 起，其中服务器受到攻击的事件共计 599145 起；可能感染病毒木马的僵尸主机共 16 台，其中确定的僵尸主机共 4 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

10 月处理网络安全事件共 2 起。其中，教育部平台通报 2 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-10-24	“漏洞盒子”安全通报一学院网站存在敏感信息泄露问题	已修复
2	2019-10-24	“教育行业信息技术工作管理平台安全监测预警子系统”安全通报，一学院公众平台发现弱密码漏洞。	已修复

3、服务器受攻击情况

本次监测时间为 10 月，服务器受到攻击事件共 599145 起；其中针对学校门户站群系统的攻击次数达到 463189 起，占总数的 77.3%。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	463189
2	地球科学在线	93801
3	中国地质大学珠宝学院	12045
4	中国地质大学(武汉)远程与继续教育学院	4113
5	实验室安全考试系统	2436
6	中国地质大学(武汉)远程与继续教育学院	2353
7	地质科技情报	2191
8	远程与继续教育学院资源管理系统	915
9	校园统一支付平台	889
10	中国地质大学(武汉)研究生管理系统	850
11	其他	16363
总计		**599145**

4、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 1355 个，中危漏洞 3024 种，低危漏洞 653 种。

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

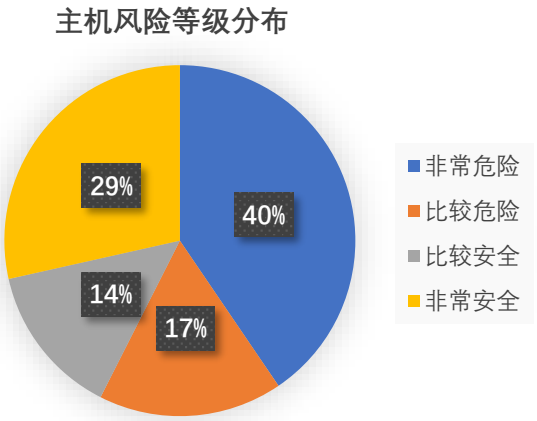
联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络中心进行复检。

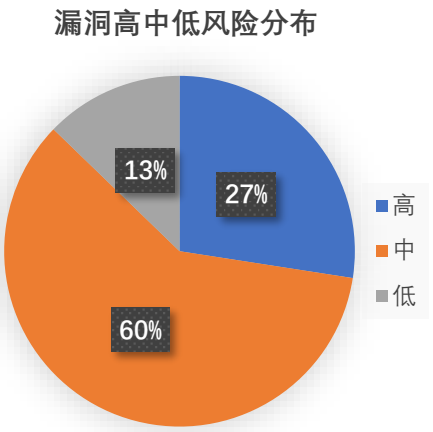
本月漏洞数量较上月基本持平，11 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网信中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
10 月份	4210	12681	5437	22328
9 月份	5030	12102	5569	22701
数量减少	820	-579	132	373

漏洞种类	主机高危	主机中危	主机低危	合计
10 月份	1355	3024	653	5032
9 月份	1378	2986	630	4994
种类增多量	-23	38	23	38

在扫描的 442 台服务器中，主机漏洞 5032 种，总计 22328 个。其中高危漏洞 1355 种，总计 4210 个；中危漏洞 3024 种，总计 12681 个；危漏洞 653 种，总计 5437 个。主机风险等级中，非常危险的占 40.5%，比较危险的占 17%，比较安全的占 14%，非常安全的占 28.5%。漏洞风险等级中，高危漏洞占比 27.4%，中危漏洞占比 59.8%，低危漏洞占比 12.8%。





5、安全漏洞整改情况

10 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。相比于 9 月，漏洞库更新，漏洞类型增多，其中主机中危漏洞增多 38 种，中危漏洞个数增多 579 个。经过整改，高危漏洞类型降低 23 种，高危漏洞个数减少 820 个，总的漏洞数量降低 373 个。

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。