中国地质大学网络安全月报

2019 年 09 月　　（第 W0043 期）（发布）　　总第 43 期

中国地质大学（武汉）网络与信息中心　　2019 年 9 月 30 日

1、情况综述

根据监测分析，9 月份我校校园网络发生的安全威胁事件共计 1419179 起，其中服务器受到攻击的事件共计 1217716 起；可能感染病毒木马的僵尸主机共 14 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 4 起，未发生重大的网络安全事件。

2、安全事件通报

9 月处理网络安全事件共 4 起。其中，教育部安全预警 2 起、教育部通报 2 起。

序号	时间	内容	处理结果
1	2019-9-11	Windows 远程桌面服务（RDP）远程代码执行漏洞预警二次更新-Apache AXIS 远程命令执行漏洞预警	已发布
2	2019-9-17	国家网络与信息安全信息通报中心对 8 个重要漏洞发布预警通告	已发布
3	2019-9-24	教育部平台通报疑似我校邮箱被盗，发送非法问题邮件	非我校资产，向教育部平台反馈
4	2019-9-26	教育部平台通报一学院网站遭黑客篡改并安装后门	已关停

3、服务器受攻击情况

本次监测时间为 9 月，服务器受到攻击事件共 1217716 起；其中针对学校门户站群系统的攻击次数达到 444375 起，占总数的 36.5%。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	站群系统	444375
2	计算机学院 CUGOJ	265420
3	网络报修系统	196123
4	站群系统	80465
5	中国地质大学 SSL VPN	27157
6	地球科学期刊服务器	26114
7	中国地质大学校友会	20373
8	地质科技情报	19854
9	中国地质大学图书馆	19409
10	采购与招标信息网	18516
11	其他	99944
总计		**1217750**

4、服务器漏洞扫描分析

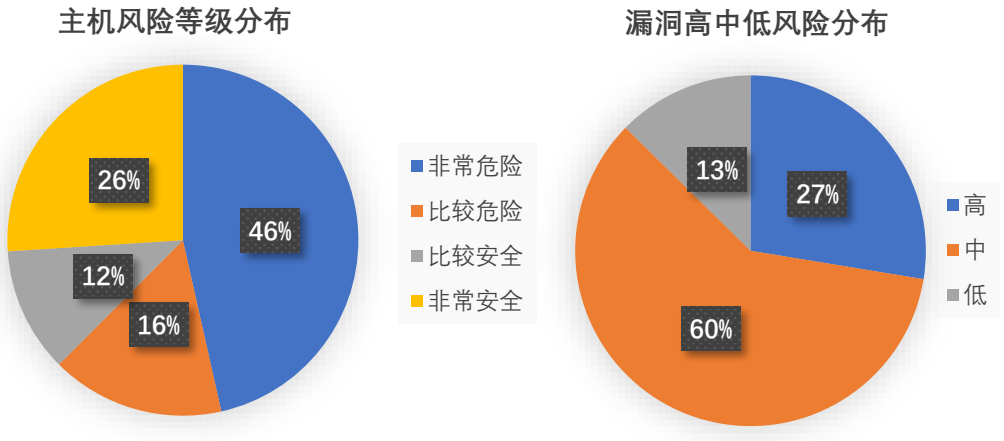
本期对校园数据中心进行漏洞扫描检测。结果统计如下：共发现高危漏洞 1379 个，中危漏洞 2986 个，低危漏洞 630 个。

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基本持平，10 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。

在扫描的 469 台服务器中，主机风险等级中，非常危险的占 46.5%，比较危险的占 16.0%，比较安全的占 11.5%，非常安全的占 26.0%。漏洞风险等级中，高危漏洞占比 27.6%，中危漏洞占比 59.8%，低危漏洞占比 12.6%。



5、安全漏洞整改情况

9 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。

9 月网信中心通过纸质通知书、电子邮件、短信提示等多种途径向各单位送达纸质版《信息系统和网站安全漏洞限期整改通知书》共计 98 份，邮件电子版 98 封，短信提醒 37 条。截止 9 月 30 日，收到《安全漏洞整改情况表》共计 52 份。对在整改期限内未收到《安全漏洞整改情况表》的信息系统和网站做关停处理。

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。