

中国地质大学（武汉）网络安全月报

2020年02月 （第W0048期） 总第48期

中国地质大学（武汉）网络与信息中心

2020年02月29日

1、情况综述

根据监测分析，2月份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，后续会继续保持和完善。

2、安全事件通报

2月处理网络安全事件共2起。其中，安全预警通报事件1起，教育系统网络安全工作管理平台通报事件1起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2月2日	关于电脑版“新型冠状病毒”的通知预警。	已通知
2	2月9日	教育系统网络安全工作管理平台安全监测预警子系统发布关于匿名者黑客扬言攻击我视频监控系统的预警提示。	已通知

3、服务器受攻击情况

本次监测时间为2月,防火墙防护服务器受到攻击事件共611747起;其中针对学校门户站群系统的攻击次数达到136841起,占总数的22.40%。门户站群系统提供我校137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	目标服务器 IP/名称	攻击次数	百分比
1	站群系统	136841	22.40%
2	中国地质大学校园虚拟专用网络服务	121697	19.90%
3	中国地质大学出版社有限责任公司(含中国地质大学出版社职教分社)	11561	1.90%
4	地球科学在线	9803	1.60%
5	校外访问平台	7965	1.30%
6	图书馆主页	7423	1.20%
7	检测数据查询	6407	1%
8	教师个人主页发布系统	5121	0.80%
9	研究生管理信息系统	4492	0.70%
10	远程教学管理平台	2684	0.40%
11	其他	297753	48.70%
12	所有	611747	100%

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:共发现高危漏洞459种,中危漏洞1663种,低危漏洞395种,漏洞种类较上月基本持平。

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

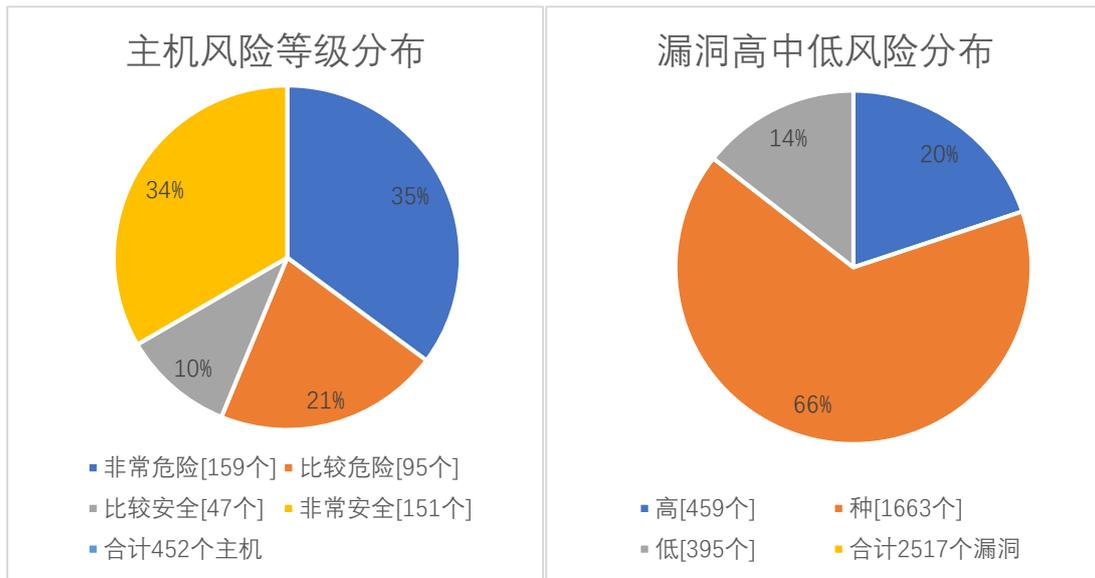
取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络与信息中心进行复检。

本月漏洞数量较上月明显减少，3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，保证正常工作作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
1月份	2995	10063	5134	18192
2月份	2510	8043	4282	14835
变化量(个)	-485	-2020	-852	-3357

漏洞种类	主机高危	主机中危	主机低危	合计
1月份	455	1689	411	2555
2月份	459	1663	395	2517
变化量(种)	+4	-27	-16	-38

在本月扫描的452台服务器中，主机漏洞共计2517种，主机漏洞总计14835个。其中高危漏洞459种，总计2510个；中危漏洞1663种，总计8043个；低危漏洞395种，总计4282个。主机风险等级中，非常危险的占35%，比较危险的占21%，比较安全的占10%，非常安全的占34%。漏洞风险等级中，高危漏洞占比20%，中危漏洞占比66%，低危漏洞占比14%。



5、安全漏洞整改情况

2月网络与信息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1月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多12327种，应用漏洞类型增多1种。根据数据分析，由于有七台主机漏洞大量减少，导致高危漏洞数量减少。

对比1月，本月高危漏洞类型增加4种，高危漏洞个数减少485个，总的漏洞类型减少38种，总的漏洞数量减少3357个。

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。