中国地质大学（武汉）校园网络安全年报

2019 年 12 月　　总第 2 期

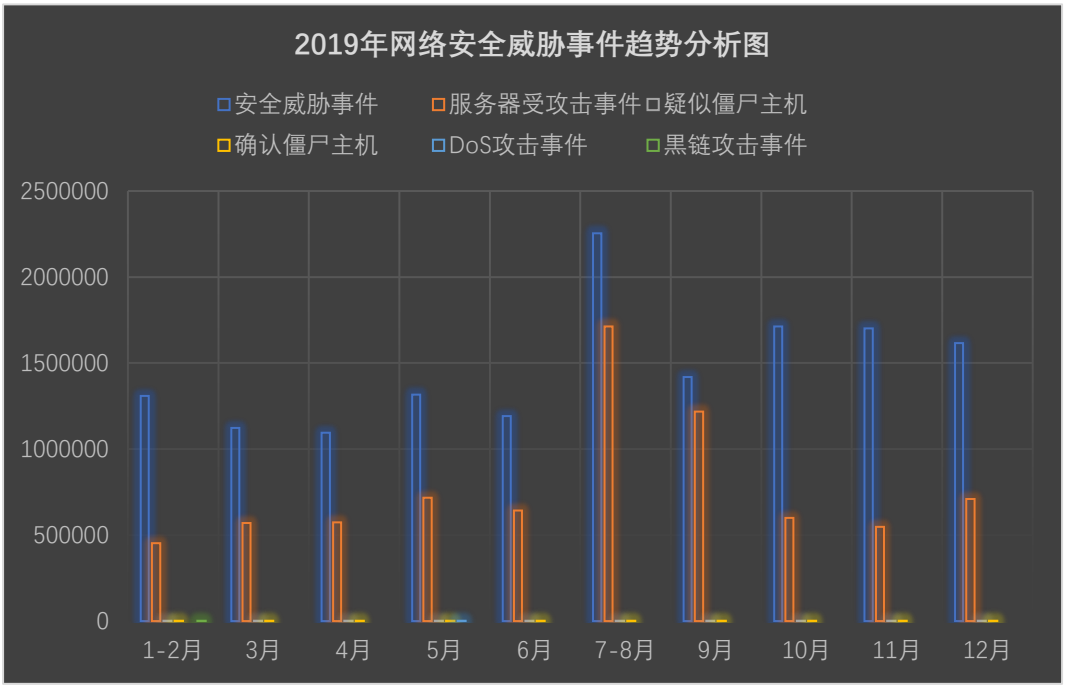
中国地质大学（武汉）网络与信息中心　　2020 年 1 月 10 日

1、情况综述

2019 年我校总体网络安全情况良好，未发生重大的网络安全事件。

根据监测分析，2019 年我校校园网络发生的安全威胁事件 14736961 起、服务器受攻击威胁事件 7742705 起、疑似僵尸主机威胁事件 268 起、确认并处理僵尸主机威胁事件 166 起、DOS 攻击威胁事件 1 起、黑链威胁攻击事件 2 起。

2019 年度网络安全威胁事件分析图



2019 年度安全监测数据统计表

月份	安全威胁事件	服务器受攻击事件	疑似僵尸主机	确认僵尸主机	DoS 攻击事件	黑链攻击
1-2 月	1309454	452281	31	24	0	2
3 月	1123157	570303	33	27	0	0
4 月	1093979	573728	36	27	0	0
5 月	1316128	717381	34	26	1	0
6 月	1191460	641796	32	26	0	0
7-8 月	2254056	1712994	42	20	0	0
9 月	1419179	1217716	14	4	0	0
10 月	1712962	599145	16	4	0	0
11 月	1701363	548099	9	4	0	0
12 月	1615223	709262	21	4	0	0

2、安全事件通报

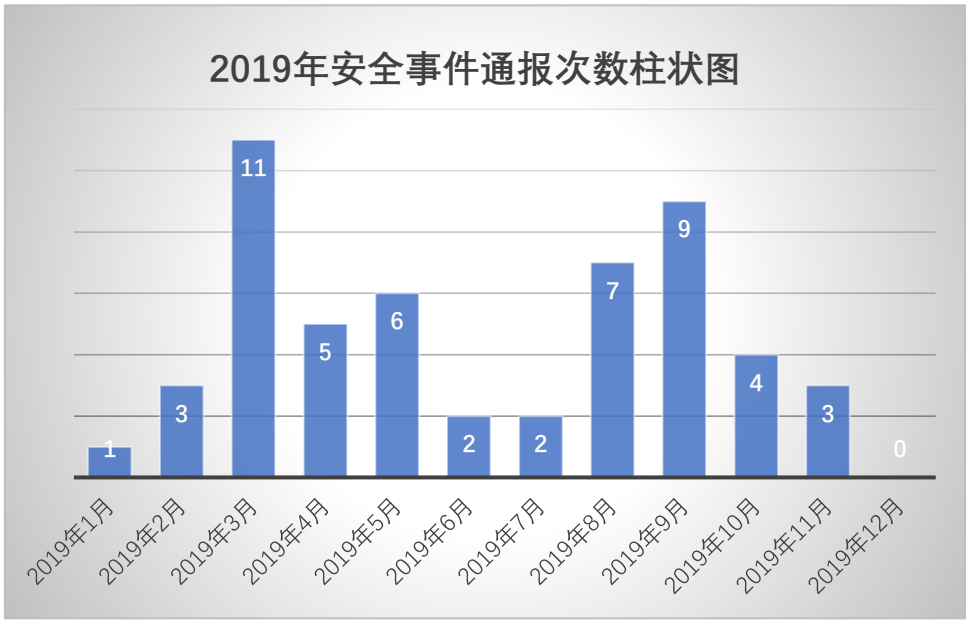
2019 年度网络与信息中心共计发布安全预警 12 次，处理网络安全通报事件 52 起：教育系统网络安全工作管理平台安全监测预警子系统通报 14 起，教育行业漏洞报告平台通报 20 起，公安机关通报 1 起，湖北省网络与信息安全通报中心通报 1 起，运营商通报 4 起，校内安全维稳及突发应急事件 12 起。

具体内容如下：

2019 年度网络安全预警明细表

时间	内容
2019 年 1 月	有关网易公司企业电子邮件系统问题通知
2019 年 3 月	教育科研网发布防范勒索病毒预警
2019 年 4 月	weblogic 反序列化安全漏洞预警
2019 年 5 月	Google 安全告警
	教育部发布 windows 漏洞预警
2019 年 6 月	关于 Absolute 公司防盗追踪软件安全风险的提示
	Coremail mailsms 接口配置读取漏洞
	关于 Coremail 邮件系统存在服务未授权访问和服务接口参数注入漏洞的安全公告
	Apache AXIS 远程命令执行漏洞预警
2019 年 8 月	微软 8 月安全补丁多个高危漏洞预警
2019 年 9 月	Windows 远程桌面服务（RDP）远程代码执行漏洞预警二次更新（CVE-2019-0708）
	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

2019 年度网络安全事件通报分析图



2018 年度网络安全事件汇总表

日期	通报单位	内容	处理结果
2019 年 1 月	教育系统网络安全工作管理平台安全监测预警子系统	某学院主页源代码泄露	已修复
2019 年 2 月	教育系统网络安全工作管理平台安全监测预警子系统	某学院主页黑链漏洞	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某单位网站 git 源代码泄露	已修复
	校内安全维稳	协助某单位处理舆情事件	已处置
2019 年 3 月	校内安全维稳	协助某单位系统排查漏洞	已处置
	教育行业漏洞报告平台	某系统存在管理员弱密码漏洞	已修复
	运营商通报	赛尔网络通报恶意域名指向	已修复
	教育行业漏洞报告平台	某学院网站敏感信息泄露	已修复
	教育行业漏洞报告平台	某学院网站敏感信息泄露	已修复
	教育行业漏洞报告平台	某学院网站敏感信息泄露	已修复
	校内安全维稳	协助某单位排查舆论事件	已处置
	教育行业漏洞报告平台	某学院网站存在 post 提交安全漏洞	已修复

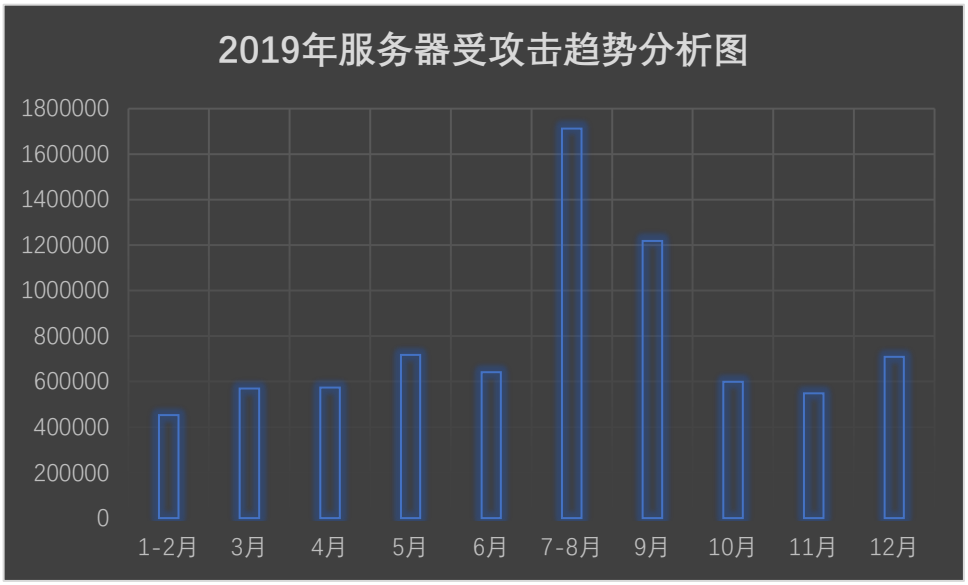
	教育行业漏洞报告平台	某学院网站敏感信息泄露	已修复
	教育行业漏洞报告平台	某学院主页验证码逻辑漏洞	已修复
2019 年 4 月	运营商通报	某单位域名备案不规范	已修复
	教育行业漏洞报告平台	某单位系统文件修改漏洞	已修复
	运营商通报	用网不规范	已修复
	教育行业漏洞报告平台	某单位网站存在 redis 未授权访问漏洞	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某学院网站个人隐私信息泄露	已修复
2019 年 5 月	教育系统网络安全工作管理平台安全监测预警子系统	某学院主页逻辑漏洞	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某学院网站隐私数据泄露	已修复
	教育行业漏洞报告平台	某网站未授权访问	已修复
	校内安全维稳	协助某单位处理舆情事件	已处置
	校内安全维稳	协助某单位处理舆情事件	已处置
	教育系统网络安全工作管理平台安全监测预警子系统	某单位主页密码管理员权限安全漏洞	已修复
2019 年 6 月	运营商通报	某学院等网站安全漏洞	已修复
	校内安全维稳	协助某单位处理舆情事件	已处置
2019 年 8 月	公安通报	洪山分局通报某学院系统漏洞	已修复
2019/7/31	教育系统网络安全工作管理平台安全监测预警子系统	某学院网站个人隐私数据泄露	已修复
2019 年 8 月	教育行业漏洞报告平台	某学院系统时间可随意更改日志访问	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某单位业务管理平台网站弱密码问题	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某学院网站存在暴力破解漏洞	已修复
	教育行业漏洞报告平台	某学院管理平台存在暴力破解漏洞	已修复
	教育行业漏洞报告平台	某学院网站弱密码	已修复

	教育行业漏洞报告平台	某学院系统信息泄露	已修复
	教育行业漏洞报告平台	某学院网站 ASP 恶意代码	已修复
2019 年 9 月	校内安全维稳	协助某单位处理舆情事件	已处置
	校内安全维稳	协助某单位处理舆情事件	已处置
	校内安全维稳	协助某单位处理舆情事件	已修复
	教育行业漏洞报告平台	自主迎新系统存在 shiro 反序列化	已修复
	教育行业漏洞报告平台	某单位系统存在 SQL 注入	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某单位系统漏洞-Shiro RememberMe 1.2.4 反序列化命令执行	已修复
	校内安全维稳	协助某单位处理舆情事件	已处置
	教育行业漏洞报告平台	疑似我校邮箱被盗，发送非法问题邮件	已修复
	湖北省网络与信息安全通报中心	某学院网站遭黑客篡改并安装后门	已修复
2019 年 10 月	校内安全维稳	协助某单位处理应急事件	已处置
	校内安全维稳	协助某单位处理舆情事件	已处置
	教育行业漏洞报告平台	某单位网站存在弱密码问题	已修复
	教育部平台安全通报	某单位网站存在弱密码问题	已修复
2019 年 11 月	教育行业漏洞报告平台	某单位系统敏感信息泄露	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某学院系统存在个人隐私泄露	已修复
	教育系统网络安全工作管理平台安全监测预警子系统	某学院网站存在 SQL 盲注入漏洞	已修复

3、服务器受攻击情况

2019 年度学校服务器受攻击事件共 7742705 起，平均月攻击次数为 645225 次，主要攻击类型网站扫描、Web 网站系统漏洞、WEBSHELL 上传、缓冲区溢出检测、SQL 注入、信息泄漏攻击。

2019 年度学校服务器受攻击趋势分析



2019 年度学校服务器受攻击次数 TOP10 服务器列表

序号	网站	受攻击次数
1	学校门户站群系统	4422105
2	计算机学院 CUGOJ	532190
3	地球科学期刊服务器	387197
4	网络报修系统	217808
5	教职工个人主页	203301
6	地质科技情报编辑部网站	159077
7	中国地质大学 SSL VPN	124471
8	图书馆服务器主页	114692
9	校办二级单位主页服务器	62703
10	网络与信息中心反向代理服务器	59476

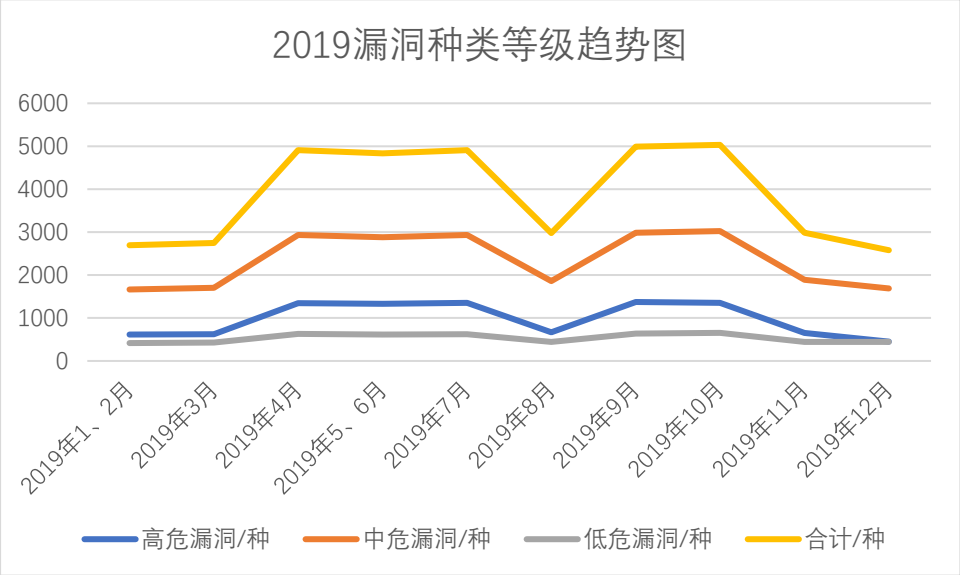
4、服务器漏洞扫描分析

2019 年针对校园网服务器漏洞扫描检测情况如下：

2019 年度漏洞种类等级分布表

时间	高危漏洞/种	中危漏洞/种	低危漏洞/种	合计/种
2019 年 1、2 月	617	1664	416	2697
2019 年 3 月	619	1700	430	2749
2019 年 4 月	1343	2934	631	4908
2019 年 5、6 月	1332	2884	615	4831
2019 年 7 月	1354	2934	621	4909
2019 年 8 月	669	1862	444	2975
2019 年 9 月	1373	2987	634	4994
2019 年 10 月	1354	3024	654	5032
2019 年 11 月	650	1890	442	2982
2019 年 12 月	450	1689	440	2579

2019 年度漏洞等级分布图



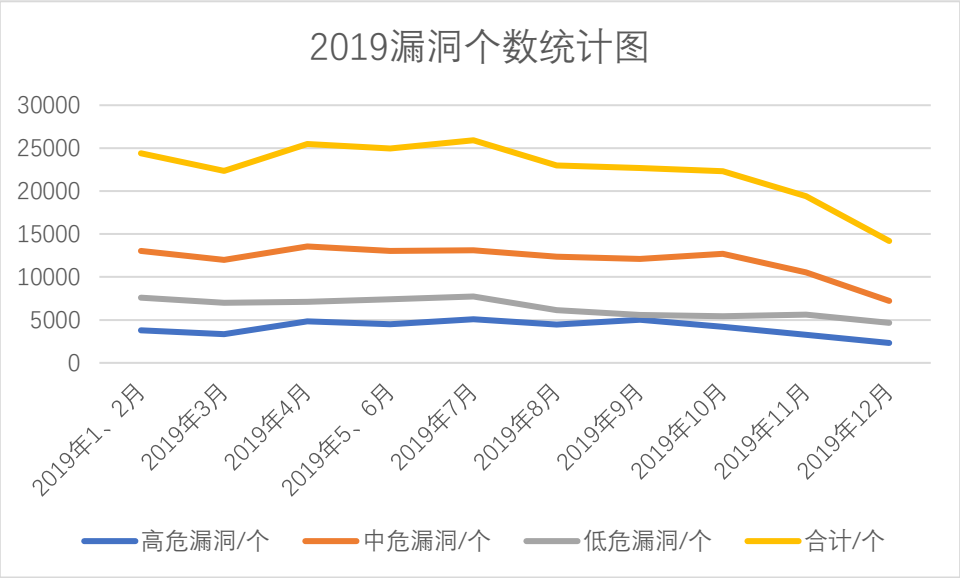
2019 年漏洞种类整体呈下降趋势，但安全形势严峻，情况不容乐观。

2019 年度漏洞个数等级分布表

时间	高危漏洞/个	中危漏洞/个	低危漏洞/个	合计/个
2019 年 1、2 月	3791	13038	7588	24417
2019 年 3 月	3356	11990	6996	22342
2019 年 4 月	4833	13556	7102	25491
2019 年 5、6 月	4496	13036	7417	24949
2019 年 7 月	5080	13110	7728	25918
2019 年 8 月	4475	12369	6140	22984
2019 年 9 月	5030	12102	5569	22701

2019 年 10 月	4210	12681	5437	22328
2019 年 11 月	3276	10530	5607	19413
2019 年 12 月	2317	7214	4660	14191

2019 年度漏洞个数等级分布图

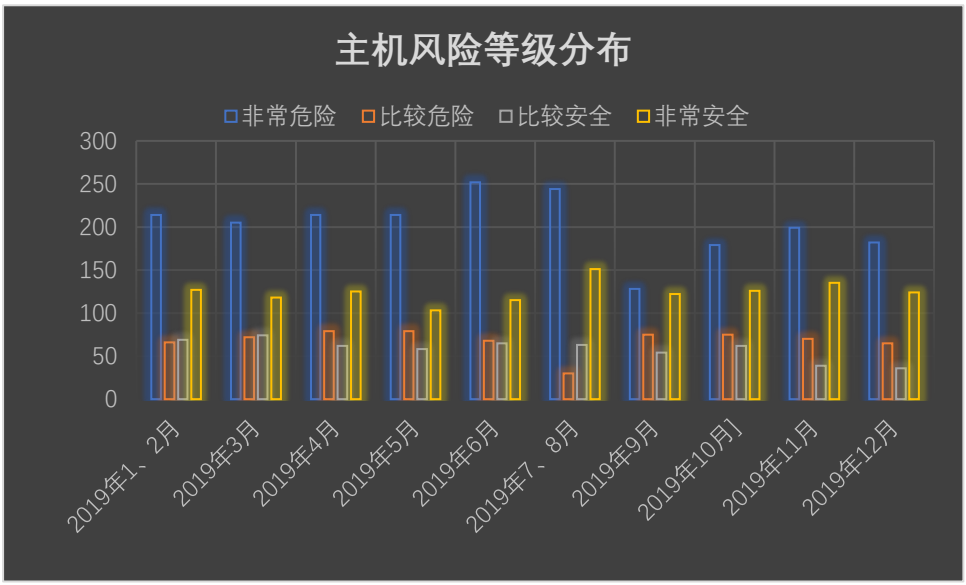


据上图数据分析，2019 年漏洞个数总体呈下降趋势，明年会继续推进漏洞整改情况，保障网站安全。

2019 年度主机风险等级分布表

时间	主机数	非常危险	比较危险	比较安全	非常安全
2019 年 1、2 月	475	214	66	69	127
2019 年 3 月	469	205	72	74	118
2019 年 4 月	480	214	79	62	125
2019 年 5 月	454	214	79	58	103
2019 年 6 月	500	252	68	65	115
2019 年 7、8 月	488	244	30	63	151
2019 年 9 月	469	128	75	54	122
2019 年 10 月	442	179	75	62	126
2019 年 11 月	443	199	70	39	135
2019 年 12 月	407	182	65	36	124

2019 年度主机风险等级分布图



黑客攻击校园网络的主要方式为漏洞攻击。网络与信息中心根据“策略放通，检测先行；逐月漏检、整改下发；认真执行、确保安全”的原则开展整改工作。通过每月进行的漏洞整改情况、漏洞检测报告的分析，结合防火墙策略控制手段，尽量将网络安全风险控制在局部，同时督促发现系统漏洞的单位按照网络与信息中心给出的整改建议尽快完成漏洞整改工作。

5、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。2019 年度共下发系统整改通知书 293 份，短信提醒督促漏洞整改工作 37 条。目前 103 个系统完成漏洞整改，其余正在逐步开展整改工作。

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。

校园网络安全隐患比较严重，全校应在管理和思想意识方面对网络安全引起足够重视。