中国地质大学（武汉）网络安全月报

2020 年 11 月　（第 W0057 期）　总第 57 期

中国地质大学（武汉）网络与信息中心　2021 年 11 月 30 日

1、情况综述

根据监测分析,11 月份我校校园网络发生的安全威胁事件共计 3898236 起，其中服务器受到攻击的事件共计 3446112 起；网站受到攻击的事件共计 452124 起;可能感染病毒木马的僵尸主机共 5 台，其中确定的僵尸主机共 12 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

11 月份我校总体网络安全情况良好，处理网络安全事件共 3 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

11 月处理网络安全事件共 3 起。其中教育系统通报安全事件 1 起，中国教育和科研计算机网通报 1 起，省委网信办通报 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	11 月 10 日	某学院机房电脑存在访问恶意 IP 问题	已整改
2	11 月 17 日	某系统存在任意文件下载漏洞。	已整改
3	11 月 26 日	某单位宣传内容表述有误。	已整改

3、服务器受攻击情况

本次监测时间为 11 月，防火墙防护服务器受到攻击事件共 3446112 起；其中针对学校门户站群系统的攻击次数达到 749321 起，占总数的 21.7%。门户站群系统提供我校 157 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	第一站群系统	749321	21.7%
2	第二站群系统	69779	2%
3	教师个人主页发布系统	50699	1.5%
4	地球科学在线	25323	0.7%
5	图书馆主页	10384	0.3%
6	地质科技情报	9821	0.3%
7	检测数据查询	6675	0.2%
8	采购管理信息系统	5027	0.1%
9	校园网 VPN 服务	4460	0.1%
10	研究生管理信息系统	4424	0.1%
11	其他	2510199	72.8%
12	所有	3446112	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：共发现高危漏洞630种，中危漏洞1714种，低危漏洞392种，漏洞种类较上月明显减少。

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。

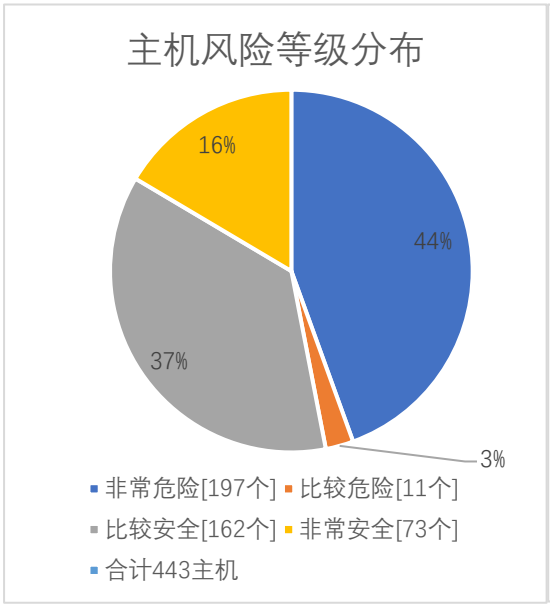
本月漏洞数量较上月明显减少，12月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

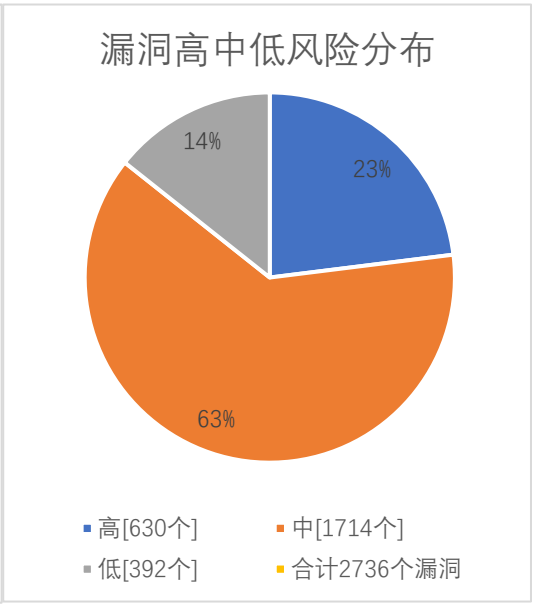
漏洞数量	主机高危	主机中危	主机低危	合计
10月份	3439	7475	3954	14868
11月份	2771	6226	3947	12944
变化量（个）	-668	-1249	-7	-1924

漏洞种类	主机高危	主机中危	主机低危	合计
10月份	655	1777	377	2809
11月份	630	1714	392	2736
变化量（种）	-25	-63	+15	-73

在本月扫描的443台服务器中，主机漏洞共计2736种，主机漏洞总计12944个。其中高危漏洞630种，总计2771个；中危漏洞1714种，总计6226个；低危漏洞392种，总计3947个。主机风险等级中，非常危险的占44%，比较危险的占3%，比较安全的占37%，非常安全的占16%。漏洞风险等级中，高危漏洞

占比 23%，中危漏洞占比 63%，低危漏洞占比 14%。





影响主机数排名前十的漏洞种类

危险程度	漏洞名称	影响主机数
高	OpenSSH 命令注入漏洞(CVE-2020-15778)	94
高	OpenSSH 安全限制绕过漏洞(CVE-2016-10012)	56
高	OpenSSH do_setup_env 函数权限提升漏洞(CVE-2015-8325)	56
高	OpenSSH auth_password 函数拒绝服务漏洞(CVE-2016-6515)	56
高	OpenSSH 多个拒绝服务漏洞（CVE-2016-10708）	56
高	OpenSSH 远程代码执行漏洞(CVE-2016-10009)	56
高	OpenSSH 安全漏洞(CVE-2016-1908)	54
高	Openssh MaxAuthTries 限制绕过漏洞(CVE-2015-5600)	54
高	OpenSSH 'schnorr.c'远程内存破坏漏洞(CVE-2014-1692)	50
高	SSL/TLS 协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	38

5、安全漏洞整改情况

11 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 10 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 1231 种，web 漏洞类型增多 10 种。11 月发放漏洞整改通知书 136 份，完成 7 个信息系统复检，总计 22 次。

对比 10 月，本月高危漏洞类型减少 25 种，高危漏洞个数减少 668 个，总的漏洞类型减少 73 种，总的漏洞数量减少 1924 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。