2020 年网络与信息系统安全月报

(12 月)

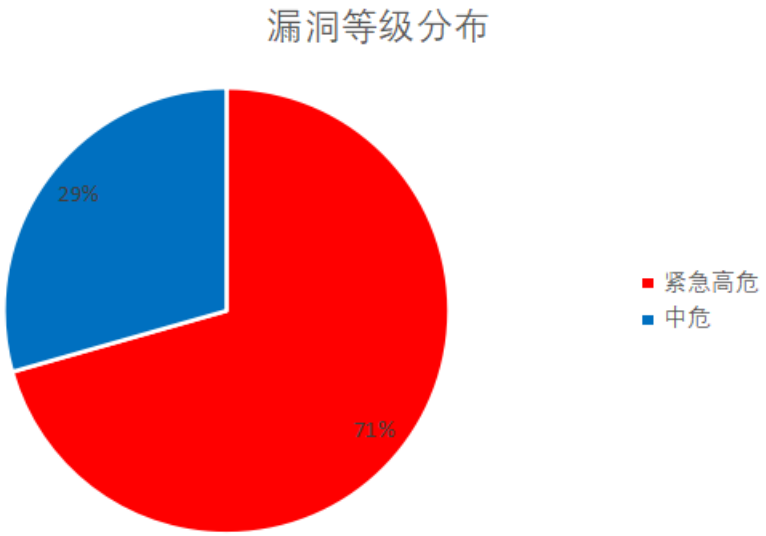
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将 12 月份网络与信息系统安全通报如下：

一、本月整体安全情况

(一) 漏洞发现情况

本月共发现漏洞 17 个。通过校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 14 个，校外通报漏洞 3 个。其中紧急高危 12 个，中危漏洞 5 个，低危漏洞 0 个，紧急高危占比：71%。紧急、高危、中危、低危漏洞统计情况见下图。



注：

紧急高危漏洞是指可远程利用并能直接获取系统权限（服务器端权限、客户端权限）或者能够导致严重级别的信息泄漏（泄漏大量用户信息或学校机密信息）的漏洞，包括但不仅限于：命令注入、远程命令

执行、上传获取 WebShell、SQL 注入、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权访问、核心业务后台弱密码等。

中危漏洞是指能直接盗取用户身份信息或者能够导致普通级别的信息泄漏的漏洞，包括但不限于目录浏览、客户端明文密码存储等。

低危漏洞是指能够导致轻微信息泄露的安全漏洞，包括但不仅限于 web 页面错误、堆栈信息泄露、JSONHijacking、CSRF、路径信息泄露、SVN 信息泄露、phpinfo 等。

(二)第三方漏洞通报情况

我校 12 月份所有第三方漏洞通报均在规定时间内完成处理，未造成网络安全事件。

漏洞通报的来源包括：教育 SRC。具体情况如下。

漏洞通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 SRC	http://202.119.243.118/	低权限账号	已修复	科学管理系统
教育 SRC	http://202.119.243.118/	高权限账号	已修复	科学管理系统
教育 SRC	http://202.119.243.118/	越权下载	已修复	科学管理系统

表一：第三方通报漏洞

(三)软件系统被入侵

本校学术期刊部投稿网站的软件系统存在程序漏洞，黑客利用此漏洞，通过上传一句话木马文件，最终实现执行植入非法链接网页文件的目的，当访客通过访问域名打开该黑页，网页会自动跳转到恶意网站。

(四)学院机房电脑感染挖矿病毒

本月通过组织安全自检扫描发现校内学院机房数台电脑被植入挖矿程序，给学校服务器的正常运行造成影响，危害校园网络安全。

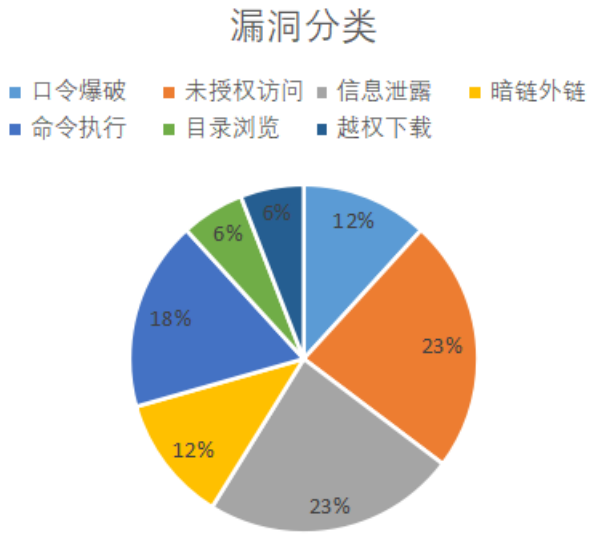
IP 地址段	部门
10.3.131.*	经济与管理学院
10.3.132.*	经济与管理学院

表二：感染挖矿病毒主机汇总表

二、安全情况分析

(一)漏洞类型分析

本月共发现漏洞 17 个。其中口令爆破 2 个，未授权访问 4 个，信息泄露 4 个，暗链外链 2 个，命令执行 3 个，目录浏览 1 个，越权下载 1 个。漏洞分类占比如下图：



(二)漏洞修复情况

2020 年 12 月共发现漏洞 17 个。其中按时修复漏洞的有 17 个。具体情况如下：

三、安全威胁风险与防范

（一）传统安全威胁风险与防范

安全威胁风险	防范措施建议
WEB 登录存在弱口令	删除登录默认密码提示，设置强密码机制并强制第一次登录修改密码。
高危服务端口未限制	启用防毒墙，在路由和防火墙做边界策略。
Windows2003 Server，Windows 2008 Server 等服务器系统漏洞。目前微软已经停止此类老旧系统漏洞补丁下载和修复服务。如果不及时升级操作系统，系统存在被入侵的隐患。	及时升级到较新版本的服务器操作系统

（二）勒索病毒（永恒之蓝）威胁风险与防范

永恒之蓝是黑客团体 Shadow Brokers（影子经纪人）2017 年 4 月 14 日公布的网络攻击工具之一，其利用 Windows 系统的 SMB 漏洞可以获取系统最高权限。不法分子通过改造“永恒之蓝”制作了 wannacry 勒索病毒，目前国内外已经出现多个高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件。

案例：2020 年富士康墨西哥的工厂服务器被入侵。黑客威胁富士

康 1804 个比特币，共计 3300 万美元(约合人民币 2.15 亿元)黑客入侵了富士康的 1200 台服务器并进行了加密，盗取了富士康 100GB 的未加密文件，并删除了 20 ~ 30TB 的备份文件。由于富士康未支付黑客在暗网的结算网站链接，黑客在暗网开始售卖富士康内部文件和业务文件。

防护手段：微软已于 2017 年发布 MS17-010 补丁，修复了“永恒之蓝”攻击的系统漏洞，用户一定要及时更新 Windows 系统补丁；务必不要轻易打开 doc、rtf 等后缀的附件；内网中存在使用相同账号、密码情况的机器请尽快修改密码，未开机的电脑请确认口令修改完毕、补丁安装完成后再进行联网操作，可以下载“永恒之蓝”漏洞修复工具进行漏洞修复。

四、网信安全每月小结

本月我校通过自检发现校内诸多主机感染病毒或存在高危漏洞，极易被不法分子利用，各单位需加强信息系统日常安全检查，定期安装或者更新病毒防护软件。全校师生要增强上网安全意识，不随意点开陌生链接或附件，做好网络安全防护。

网络与信息系统安全联系电话：58139275,83172363。

信息服务部

2021 年 1 月 5 日