

2023 年网络与信息系统安全月报 (10月)

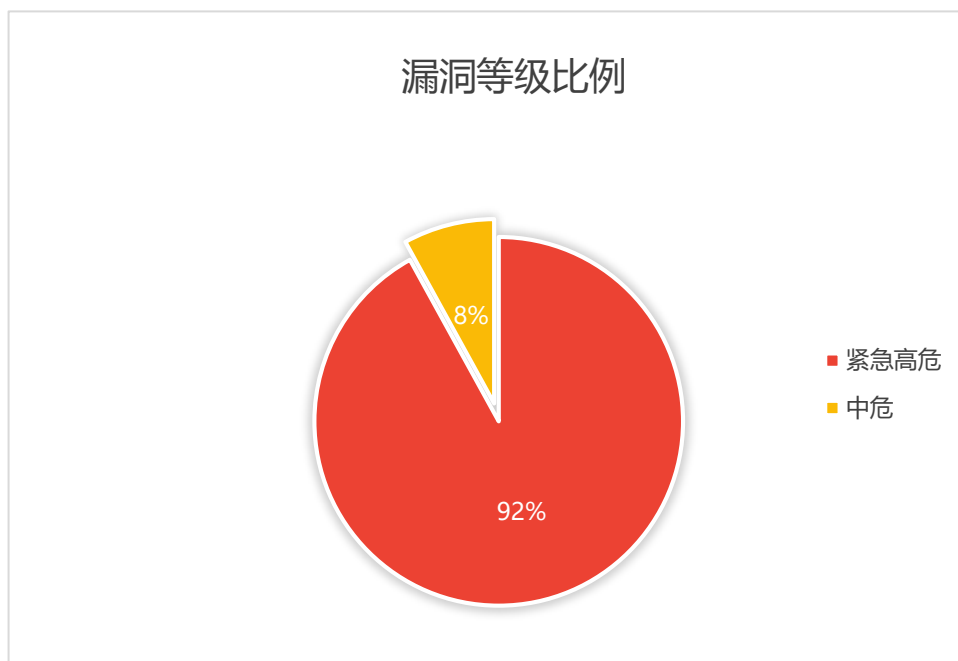
各单位、部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将10月份网络与信息系统安全情况通报如下：

一、本月整体安全情况

(一) 漏洞发现情况

本月共发现漏洞 13 个。通过在校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 13 个，校外通报漏洞 0 个，外链 0 个。其中紧急高危 12 个，中危漏洞 1 个，低危漏洞 0 个，紧急高危占比：92%。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

本月未收到第三方漏洞通报。

（三）非法外链情况

本月未检查到我校所属网站存在非法外链。

（四）省教育网信办网络安全现场检查

10月30日，江苏省教育网信办对我校网络安全情况进行了现场检查，对我校网络安全工作部署、网络安全责任制落实、网络安全法律法规要求落实、网络安全重点措施落实和数据安全工作开展等方面的工作材料进行了查阅，并通过漏洞扫描、配置核查和渗透测试等方式对我校网络内网环境和重要信息系统进行了现场检查。

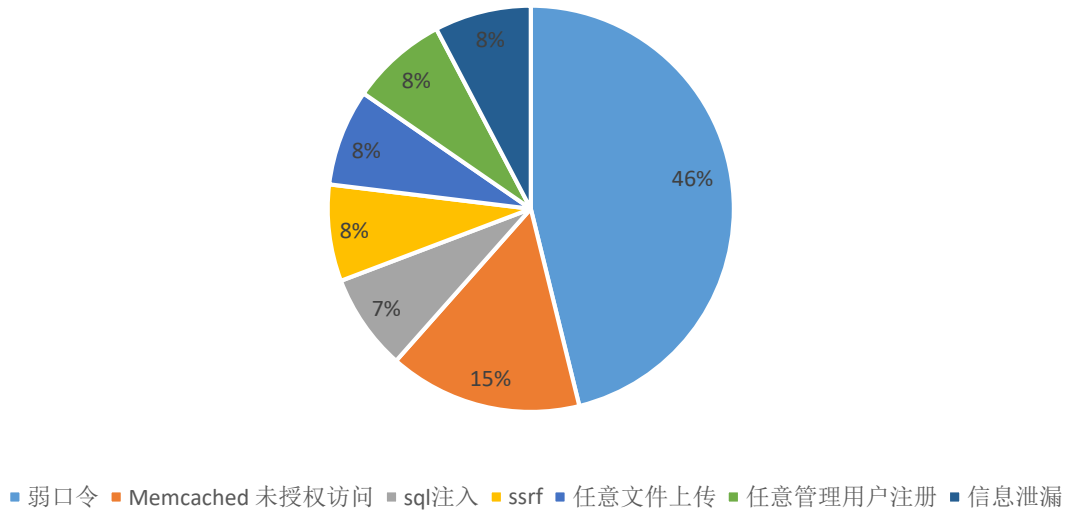
本次检查发现我校校园网内网部分信息系统存在漏洞，漏洞类型为弱口令和未授权访问，查出的漏洞已经及时完成修复。本次检查进一步摸清了我校网络安全防护现状，检验和提升了我校网络安全防护能力。

二、安全情况分析

(一) 漏洞类型统计

本月共发现漏洞 13 个。其中弱口令 6 个，Memcached 未授权访问 2 个，sql 注入、ssrf、任意文件上传、任意管理用户注册、信息泄漏各 1 个。漏洞分类占比如下图：

漏洞分类



(二) 漏洞修复统计

本月共发现漏洞 13 个，均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
弱口令较多	加强人员网络安全防范意识，定期修改网站登录密码。
网页存在暗链外链	定期排查网页外链，清除过期链接，避免被恶意抢注为非法网站。

网站未授权访问	加强厂商人员网络安全防范意识，对各自应用系统目录的访问权限严格排查。
---------	------------------------------------

四、网信安全每月小结

本月我校信息系统漏洞总数量较少，因各部门响应处理及时，未造成网络安全事件。本月我校安全漏洞主要集中在未授权及弱口令等方面。各单位需定期修改登录口令，加强网络安全防范意识，以更强烈的担当、更主动的作为、更严实的作风、更有力的措施，把学校的网络安全保障工作抓紧做实，齐心协力共同筑牢网络安全工作防线。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023年11月8日