网络与信息安全情况通报

第 11 期

丽江市网络与信息安全监测预警通报中心　　2020 年 5 月 19 日

目　录

一、关于防范境外黑客组织借“两会”话题对我市实施网络攻击的预警通报

近日，国家网络与信息安全信息通报中心监测发现，有境外黑客组织企图借全国“两会”话题对我党政机关、政府部门工作人员实施网络钓鱼攻击。经分析研判，攻击者仿冒QQ邮箱中转站页面，并放置涉“两会”话题诱饵文档，妄图窃取我政府部门相关邮箱账号密码等敏感信息，开展情报收集。

目前，全国“两会”召开在即，请各单位高度重视，立即采取以下防范措施：**一是**提高警惕，加强防范，不要随意点击未知链接，切勿打开不明来历的文件、电子邮件；**二是**要加强网络安全隐患自查和系统加固工作，提高系统和数据安全保护能力；**三是**严格落实值班值守制度，做好应急处置准备，如发现网络攻击情况，要及时与属地公安机关网安部门联系，在公安机关网安部门的指导下进行处置。

二、关于启明星辰运维安全网关存在高危漏洞的预警通报

近日，国家网络与信息安全信息通报中心监测发现，启明星辰公司天玥运维安全网关产品存在多个高危安全漏洞，该产品主要用于网络设备、安全设备、主机系统及数据运维管理，广泛应用于国内电子政务云以及大中型国有企业和政

府机构。经分析研判，上述设备存在文件读取、SQL 注入、越权查看、存储型跨站脚本攻击等高危安全漏洞，攻击者在获取管理员权限或运维用户权限的情况下，可利用上述漏洞，查看敏感数据，实施网络攻击。受影响产品固件版本号为 6.0.7.11033。

目前正值疫情防控和“两会”安保的关键时期，请各单位高度重视，立即采取以下防范措施：**一是**立即对本单位及下属单位是否使用启明星辰公司天玥运维安全网关产品进行梳理排查，组织使用该产品的单位、部门及时升级固件版本，消除安全隐患。5 月 16 日 12 时启明星辰公司已正式发布补丁程序，请涉及单位及时联系该公司官方客服（4006243900、01056632600），获取补丁程序。**二是**加强管理员和运维用户账号密码管理，立即将登录密码更改为强口令（8 位以上，包括大小写字母、特殊符号和数字）并定期更换。**三是**及时开展隐患排查和安全加固工作，若发现攻击情况，要完整固定保留有关记录，及时与属地公安网安部门联系，在公安网安部门的指导下进行处置。

请各网安大队将该通报情况及时报分管领导。并及时将此通报转发本地信息通报机制成员单位，组织有关单位开展梳理摸排和漏洞修复工作，有关工作情况于 2020 年 5 月 22 日 12 时前报支队（通报中心）。

送：市直各委、办、局

市级各重要信息系统运营使用单位及行业主管部门。

抄：市公安局警令部，科信处，县（区）网安大队。