中共北京市委网络安全和信息化领导小组办公室

关于紧急开展网络安全漏洞排查工作的通知

各委办局、各区：

2017年3月7日，Apache Struts 2软件被曝远程命令执行高危漏洞（已得官方确认），漏洞编号S2-045，CVE编号CVE-2017-5638。该漏洞是基于 Jakarta plugin 插件的Struts远程代码执行漏洞，黑客可通过Jakarta文件上传插件实现远程利用该漏洞执行代码，在上传文件时通过修改HTTP请求头中的Content-Type值来触发该漏洞，进而执行系统命令。该漏洞影响范围为 Struts2.3.5-Struts2.3.31、Struts2.5-Struts 2.5.10，升级Struts到Struts2.3.32或Struts2.5.10.1版本可修补该漏洞。该漏洞危害程度极为严重，可直接获取应用系统所在服务器的控制权限，请各单位高度重视。

Apache Struts 2是世界上最流行的Java Web服务器框架之一，普遍应用于互联网、政府和企业门户网站，特别是互动性较强的用于报名、注册、查询、留言的信息系统。当前，全国“两会”正在顺利召开，我市网络安全保障工作处于关键阶段，针对这一突发情况，市委网信办紧急召集公安、经信等网络安全管理部门及相关技术专家进行分析研判。为切实保障我市党政机关及国有企事业单位网站安全，现提出以下要求，请相关部门及网站遵照执行。

（一）请市公安局、市经信委、市安全局等我市网络安全管理部门加强技术监测检查，发现有关漏洞情况及时下发整改通知，督促、指导整改措施落实到位。

（二）请市经信委协调安排相关政府部门网站开展自查，及时发现修复漏洞，同时要对服务器主机进行木马病毒扫描，防止相关漏洞已经被利用并植入恶意程序，切实杜绝安全隐患。

（三）请市国资委、市委教育工委、市教委、市卫计委等单位监督指导各下属企业、院校、医疗等国有企事业单位网站进行有关漏洞的专项检查并彻底清除安全隐患。

（四）各党政机关及企事业单位应及时将检查发现的漏洞及修复情况报送市委网信办（传真：67196600）。

中共北京市委网络安全和信息化领导小组办公室

2017年3月8日

（联系人：杨虎　　电话：010-67196557）