**（紧急）勒索病毒及Winrar、KindEditor漏洞预警**

一、勒索病毒预警

近期，勒索病毒呈高发态势，网警支队发现勒索病毒最新变种GandCrabv5.1疑似通过控制的单位内网办公终端，扫描局域网服务器，利用服务器远程桌面3389端口投放勒索病毒，成功入侵服务器后，加密受害机器上超过400种类型的数据文件。

建议各单位：及时给办公终端的操作系统以及第三方应用打补丁修复漏洞，并安装终端安全防护软件；业务服务器除了安装杀毒软件还需要部署安全加固软件，阻断黑客攻击；应采用足够复杂的登录密码登录办公系统或服务器，并定期更换密码，严格避免多台服务器共用同一个密码；对重要数据和核心文件及时进行备份，并且备份系统与原系统隔离，分别保存；增加全流量威胁检测手段，实时监测威胁、事件；应尽量关闭不必要的常见网络端口，比如：445、3389等；提高安全运维人员职业素养，除工作电脑需要定期进行木马病毒查杀外，如有通过VPN接入远程办公电脑也需要定期进行病毒木马查杀。

二、WinRAR目录穿越漏洞

WinRAR 是一款功能强大的压缩包管理器，它是档案工具RAR在Windows环境下的图形界面。2019年 2 月 20 日国外安全研究人员发布了Winrar一个严重漏洞，当用户解压压缩包时可以导致命令执行，目前官方已经推出beta版修复该漏洞。影响版本：Winrar <= 5.61的版本均受影响。

修复建议： 将Winrar升级成5.70Beta 1,或使用其他非unacev2.dll动态链接库来处理ace压缩包的压缩软件。

三、KindEditor上传漏洞

近日，监测发现近百起党政机关网站被植入色情广告页面，分析发现被植入色情广告页面的网站都使用了KindEditor编辑器组件，我市也有部分单位受到影响。本次安全事件主要由upload\_json.\*上传功能文件允许被直接调用从而实现上传htm,html,txt等文件到服务器，在实际已监测到的安全事件案例中，上传的htm,html文件中存在包含跳转到违法色情网站的代码，攻击者主要针对党政机关网站实施批量上传，建议使用该组件的网站系统尽快做好安全加固配置，防止被恶意攻击。影响版本：KindEditor<= 4.1.11的版本的版本均受影响。

修复建议：本次漏洞级别为高危，目前针对该漏洞的攻击活动正变得活跃，建议尽快做好安全加固配置。

**安全运营方面建议：**直接删除upload\_json.\*和file\_manager\_json.\*即可。

**安全开发生命周期（SDL）建议：**KindEditor编辑器早在2017年就已被披露该漏洞详情，建议网站建设单位经常关注其系统使用的框架、依赖库、编辑器等组件的官方安全更新公告。