



网络安全风险预警

2023 年第 3 期（总第 19 期）

广西大学网络信息中心 2023 年 9 月 26 日

【预警类型】 高危预警

【预警内容】

关于 WPS Office 和 QQ Windows 客户端存在远程代码执行漏洞的预警通报

一、漏洞概述

WPS Office 个人版存在远程代码执行漏洞，攻击者可利用该漏洞生成恶意文档，受害者打开文档可被执行恶意代码，导致设备被远程控制；

QQ Windows 客户端存在远程代码执行漏洞，攻击者利用漏洞可通过转发消息传播恶意代码，在被攻击者点击消息内容时，恶意代码将被自动下载执行。

二、漏洞影响范围

WPS Office 受影响版本：

WPS 个人版 12.1.0.15355 及之前版本。

QQ Windows 受影响版本：

Windows 版 QQ 9.7.13 及之前版本。

三、漏洞处置建议

目前，金山和腾讯公司均已发布在线升级补丁和安全版本修复漏洞。

请各部门单位高度重视，升级版本修复漏洞，并警惕钓鱼风险，不打开来源不明的文件，不点击聊天窗口的不明网络链接。如遇紧急情况，及时与信息网络中心联系，联系电话：0771-3236514。

处置参考链接：

1. <https://platform.wps.cn/2023/>

2. <https://im.qq.com/pcqq>