**关于蓝牙(Bluetooth)协议存在多个漏洞的安全公告**

物联网安全研究公司Armis Labs披露了一个新的攻击方法，主流操作系统包括Android、iOS、Windows、Linux系统的设备均受其影响。攻击者通过蓝牙(Bluetooth)协议远程不经过任何传统网络介质发起攻击，可以控制设备，突破访问企业数据和网络，向横向相邻的设备传播恶意软件，极有可能导致大规模蠕虫的跨网攻击。相关漏洞详情如下：



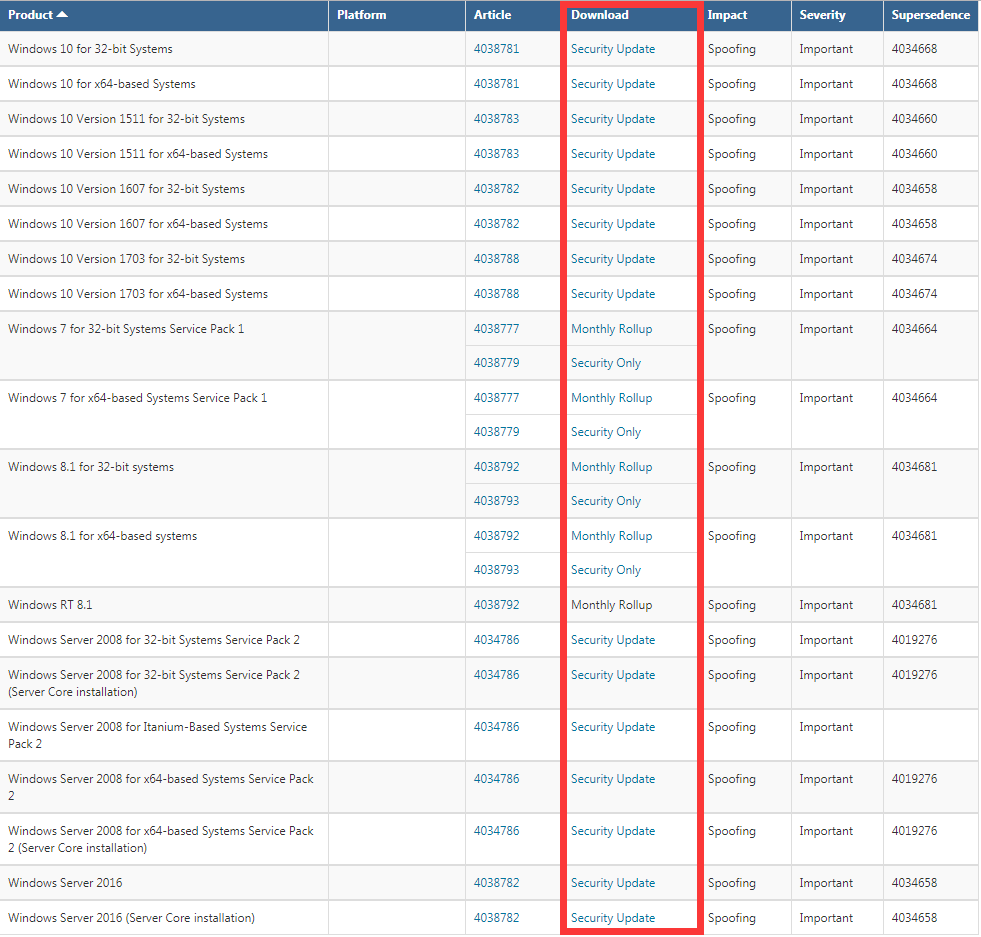
解决方法

1、苹果终端升级iOS版本至9.3.5以上

2、安卓终端升级Android版本至6.0以上

3、Windows终端根据版本下载并安装相应安全补丁：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628>

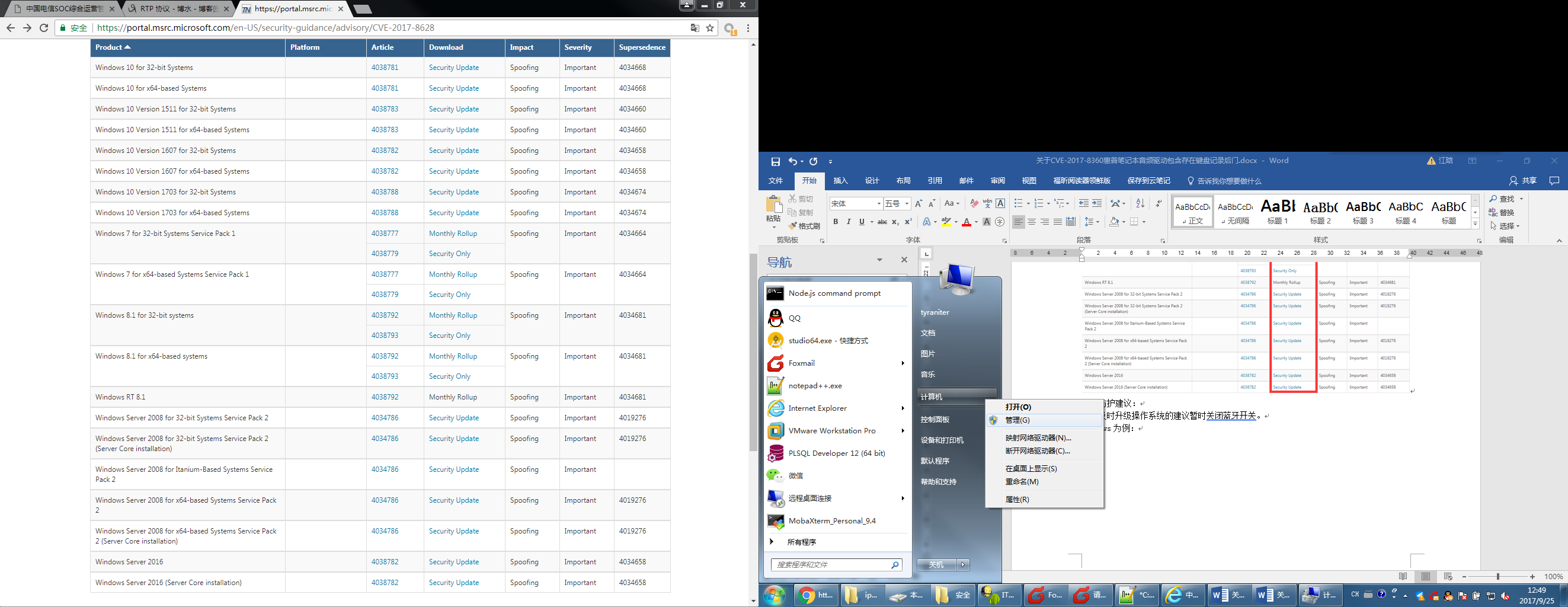


临时防护建议：

不能及时升级操作系统的建议暂时关闭蓝牙开关。

Windows为例：

开始-计算机-右键-管理-设备管理器



对于蓝牙条目下的所有设备-右键-禁用

