卓又现新毛病 41%装备可通过Wi-Fi网络被攻击

Android 6.0及以上版本系统都存在这个毛病，研究职员表现由于基数过大，因此在利用和阻挡Linux和Android装备时天生的流量很容易被忽略，有41%的安卓装备都很是容易遭受到这种“具有扑灭性”的无线网络攻击。通过攻击黑客可以入侵网站，嵌入勒索或恶意软件，安卓装备需要通过宁静补丁更新的方式才气免受攻击。

通过阻挡通讯可以让攻击者读取我们以为宁静的加密信息，黑客甚至不需要破解Wi-Fi密码就能实现这一目的。这个毛病需要装备处于恶意攻击的有用规模之内，可以被用来窃守信用卡卡号、密码、谈天信息、照片、电子邮件以及在线通讯工具内容。

只管大多数的装备看起来都是容易受到攻击的目的，但这种攻击方式是通过读取无线网络流量的方式实现，而并不针对接入点。该攻击使用了WPA2协议4-way
handshake的毛病，后者是一种确保客户端和会见点在加入无线网络时使用相同密码的宁静协议。

腾讯科技讯 10月16日据外洋媒体报道，最近又泛起了一个新毛病，可以让攻击者在联网装备和无线接入点之间读取到无线通讯协议，甚至还能将其修改，把恶意软件嵌入到网站中。研究职员今天正式对外披露了这项毛病，而且表现安卓和基于Linux系统的装备受到的影响最大。这种攻击对所有使用WPA或WPA 2加密的Wi-Fi网络都生效，而且其最大的弱点就是Wi-Fi尺度自己，因此包罗macOS、Windows、iOS、Android和Linux理论上都有可能受到攻击。

由于这是一种基于客户机的攻击，预计未来几周会陆续有更新补丁泛起。研究职员在七月份就已经提前向特定的硬件厂商发出了通知，而且在八月下旬公布了周全的提醒。宁静研究职员表现，用户无需更改Wi-Fi密码，由于这并不能阻止攻击的发生，但建议路由器和所有的客户端装备都安装最新的宁静补丁。（编译/音希）

它还需要一个滋生和孕育的土壤，暂时的落后，并意味着停止了追赶的脚步。

夜色中，全新设计的头尾灯更为C级车赋予了独有的、识别力极高的迷人外观，车尾示廓灯和刹车灯同样采用相同的LED技术。