防范智能家居设备安全风险　趋势科技建议从路由器入手

黑客可通过攻击路由器取得设备控制权　窃取用户隐私数据

[趋势科技中国]– [2015 年 7 月 29 日] 为了让生活更加轻松，现在很多家庭都安装了智能家居设备。但无论是智能摄像头、智能灯泡，还是其它智能家居设备都存在着安全风险，并可能会危及你的隐私。由于很多智能设备缺乏严密的安全机制，恶意分子能够更加轻易地破解用户认证并访问网页和操作界面，从而获取用户的隐私信息。近日，趋势科技发现，智能家居设备中的安全漏洞为网络犯罪分子大开方便之门，通过这些漏洞，网络犯罪分子能读取其中的机密数据，甚至控制这些智能家居设备。在 2014 年时，著名的 Shellshock 漏洞就影响了包括智能灯泡在内的许多设备。

趋势科技（中国区）资深产品市场经理徐江明指出：“要防御黑客对智能家居设备的攻击，最好从路由器入手，因为这往往是恶意分子入侵网络的首选目标。一旦被取得路由器的控制权，他们就能够监视和影响你的设备与线上活动。但可悲的是，只有少数用户知道路由器其实很脆弱，因为它们是用户暴露在互联网上的‘据点’，黑客可以通过攻击路由器来获得网络的控制权。”

在某些情况下，路由器可能会出现一些看似不起眼的固件 BUG，但黑客已经可以通过这些 BUG 来攻击系统并取得系统权限。**为了尽量减少路由器所遭受的攻击，加强家用路由器安全，趋势科技为建议用户：**

- **改变默认的管理设定**：因为管理者权限和密码是攻击者尝试破解的第一目标。
- **使用加密措施**：打开路由器设置界面来启用 WEP 或 WPA，并输入密码以生成加密的密钥来加强安全性，并确保这些密码不会被泄露到外界。
- **停止使用与远程控制相关的功能**：该功能可以让你不在家时进行远端管理和使用 FTP。但这会让管理界面暴露在网络上。如果你需要将其打开，确保使用 HTTPS 进行远端管理和启用适当的限制。
- **定期更新固件**：如前所述，漏洞的 BUG 会让你的路由器容易遭受攻击。为了防止这种情况，请确保你的固件保持在最新状态。
- **启用路由器的防火墙**：虽然路由器通常默认启用此项功能，但你仍应该检查此项设置以确保路由器在防火墙的保护之中。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商 ,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问: www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。