2017 年 11 月 20 日，星期一

这个假日季 - 购买一台物联网设备即可获得免费通用漏洞披露 (CVE) 服务

随着物联网变得炙手可热并不断发展，攻击者和影响这些系统的威胁也在持续涌现。世界各地的公司都在忙于部署连接互联网的低成本计算设备（又名物联网）来解决业务问题并改善我们的生活。同时，犯罪分子也在不断开发新的方法来利用和危害易受攻击与防御不足的设备。

在过去的一年里，我们看到犯罪分子利用易受攻击的物联网设备来构建 Mirai 僵尸网络，得以发起历史上最大的拒绝服务攻击，而且最近我们发现了更多的物联网僵尸网络，涉及数千台被感染并为犯罪分子执行命令的设备。攻击者可以向这些设备网络发送命令，攻击网站，同时利用大量网络流量造成协同拒绝服务攻击，使系统崩溃。

Talos 团队研究并监测威胁环境，以帮助思科客户抵御新型威胁。我们努力使更广泛的社区认识到不安全的物联网设备所带来的问题，并积极寻找漏洞。最近几周，Talos 团队发布了关于我们已解决的一些漏洞的若干报告，其中包括在家庭安全摄像头（一款用于提高安全性的迪斯尼品牌家庭物联网设备）中发现的漏洞，以及在嵌入式系统中运行的软件（比如一些物联网系统使用的软件）中发现的漏洞。

其中许多漏洞使攻击者能够在设备上执行未经授权的计算机代码，从而可以读取数据，对其他系统发起攻击，或使被感染的设备无法运行。不仅不安全的设备会泄露应永远保密的信息，而且存在漏洞的设备若未获得保护，还会被攻击者利用。

与对待 Talos 团队发现的所有漏洞一样，我们遵循我们所发布的漏洞披露责任政策，确保供应商有时间发布补丁程序以修复漏洞。我们知道在这一领域中，对易受攻击的系统应用补丁程序并不简单，有时甚至无法实现。正因如此，当我们披露存在的漏洞时，会发布开源 Snort 签名来检测和阻止利用漏洞的企图。

通过入侵防御系统 (IPS) 网络安全防御功能来保护可能易受攻击的物联网设备仅仅是思科提供的全套物联网保护的一部分。思科还通过思科网络技术学院提供网络安全和物联网培训课程。这些计划的目标是提高在职员工的技术水平，并使新员工能够掌握步入职场，取得成功所需的知识。

保护物联网首先需要从认识问题开始。认识到问题和风险并提出解决方案是解决问题至关重要的首要步骤。我们致力于在我们的研究中找出犯罪分子用来破坏物联网的漏洞和方法，并致力于确保每个人都能获得这一新的前沿服务所带来的好处。

发布者：MARTIN LEE，发布时间：12:14 PM

标签：物联网、漏洞