2016年IOT设备漏洞情况统计简报(CNVD)

近年来，随着智能手机、可穿戴设备、活动追踪器、无线网络、智能汽车、智能家居等终端设备和网络设备的迅速发展和普及利用，针对IOT设备的网络攻击事件比例呈上升趋势，攻击者利用IOT设备漏洞可导致设备拒绝服务、获取设备控制权限进而形成大规模恶意代码控制网络，或用于用户信息数据窃取、网络流量劫持等其他黑客地下产业交易。国家信息安全漏洞共享平台（以下简称CNVD）对2016年收录的IOT设备漏洞（含通用软硬件漏洞以及针对具体目标系统的事件型漏洞）进行了统计，相关情况简报如下:

一、IOT设备通用漏洞按厂商排名

2016年CNVD收录IOT设备漏洞1117个，漏洞涉及Cisco、Huawei、Google、Moxa等厂商。其中，传统网络设备厂商思科（Cisco）设备漏洞356条，占全年IOT设备漏洞的32%；华为（Huawei）位列第二，共收录155条；安卓系统提供商谷歌（Google）位列第三，工业设备产品提供厂商摩莎科技（Moxa）、西门子（Siemens）分列第四和第五。

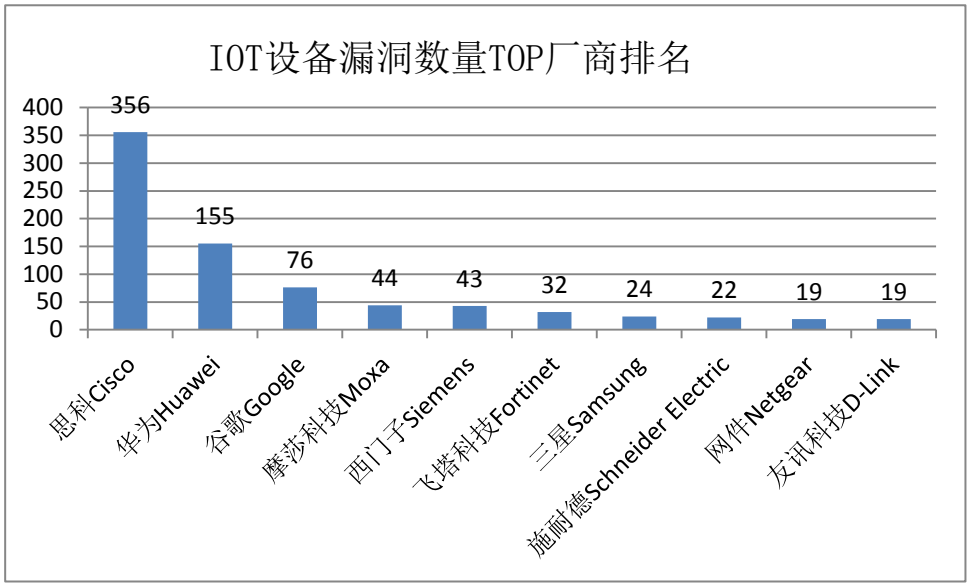

图 1 IOT设备漏洞数量TOP厂商排名(来源：CNVD)

二、IOT设备通用漏洞按风险技术类型分布

2016年CNVD收录IOT设备漏洞类型分别为权限绕过、拒绝服务、信息泄露、跨站、命令执行、缓冲区溢出、SQL注入、弱口令、设计缺陷等漏洞。其中，权限绕过、拒绝服务、信息泄露漏洞数量位列前三，分别占收录漏洞总数的23%，19%，13%。而对于弱口令（或内置默认口令）漏洞，虽然在统计比例中漏洞条数占比不大（2%），但实际影响却十分广泛，成为恶意代码攻击利用的重要风险点。

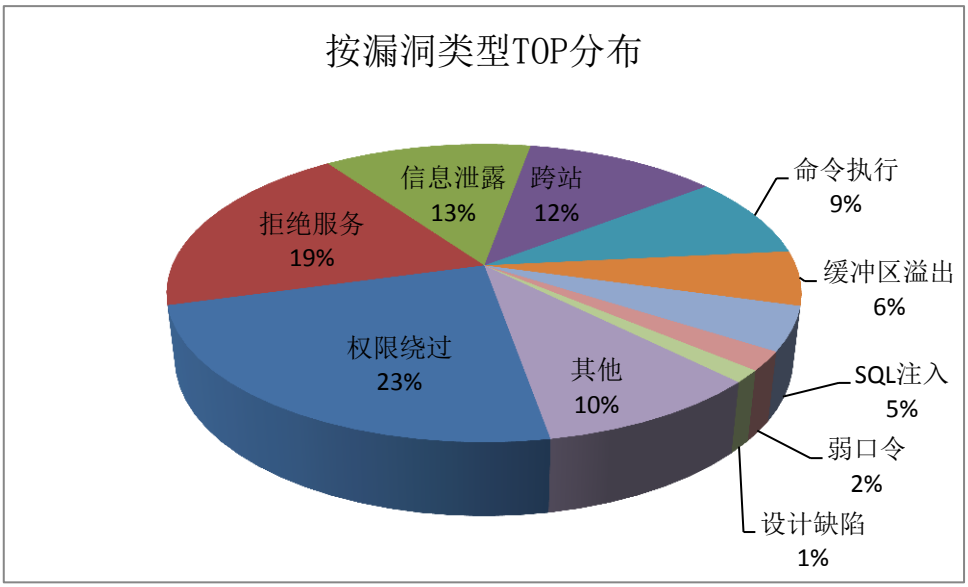

图 2 按漏洞类型TOP分布

三、IOT设备通用漏洞按设备标签类型分布

2016年CNVD公开收录1117个IOT设备漏洞中，影响设备的类型（以标签定义）包括网络摄像头、路由器、手机设备、防火墙、网关设备、交换机等。其中，网络摄像头、路由器、手机设备漏洞数量位列前三，分别占公开收录漏洞总数的10%，9%，5%。

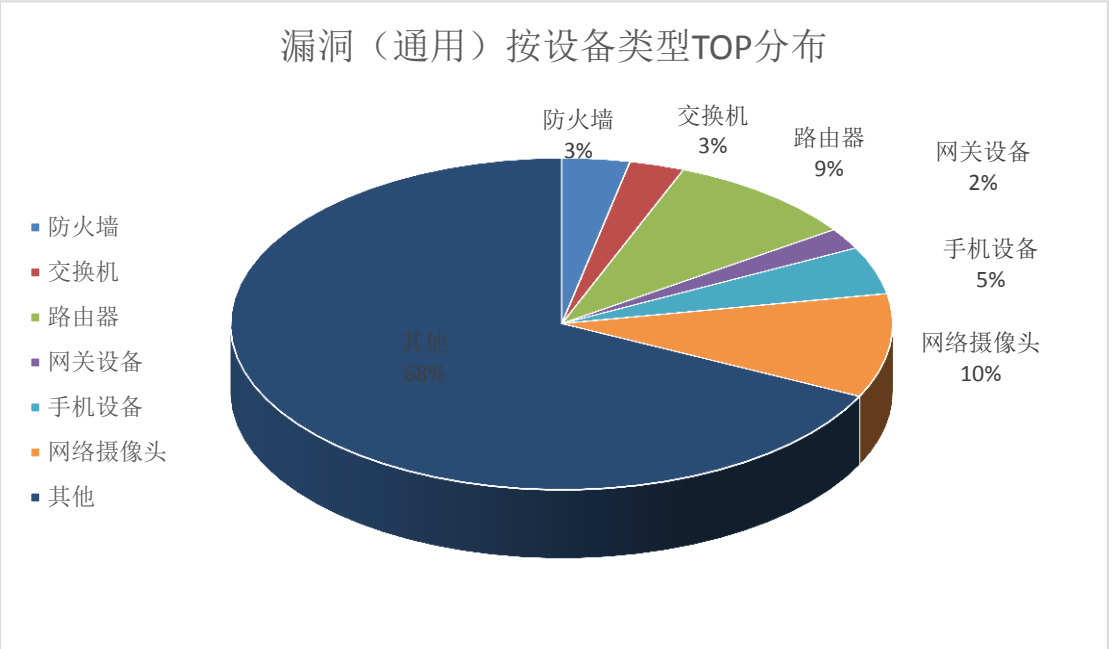

图 3 漏洞（通用）按设备类型TOP分布（来源：CNVD）

四、IOT设备事件型漏洞按设备标签类型分布

根据CNVD白帽子、补天平台以及漏洞盒子等来源的汇总信息，2016年CNVD收录IOT设备事件型漏洞540个。与通用软硬件漏洞影响设备标签类型有所不同，主要涉及交换机、路由器、网关设备、GPS设备、手机设备、智能监控平台、网络摄像头、打印机、一卡通产品等。其中，GPS设备、一卡通产品、网络摄像头漏洞数量位列前三，分别占公开收录漏洞总数的22%，7%，7%。值得注意的是，目前政府、高校以及相关行业单位陆续建立一些与交通、环境、能源、校园管理相关的智能监控平台，这些智能监控平台漏洞占比虽然较少（2%

），但一旦被黑客攻击，带来的实际威胁却是十分严重的。

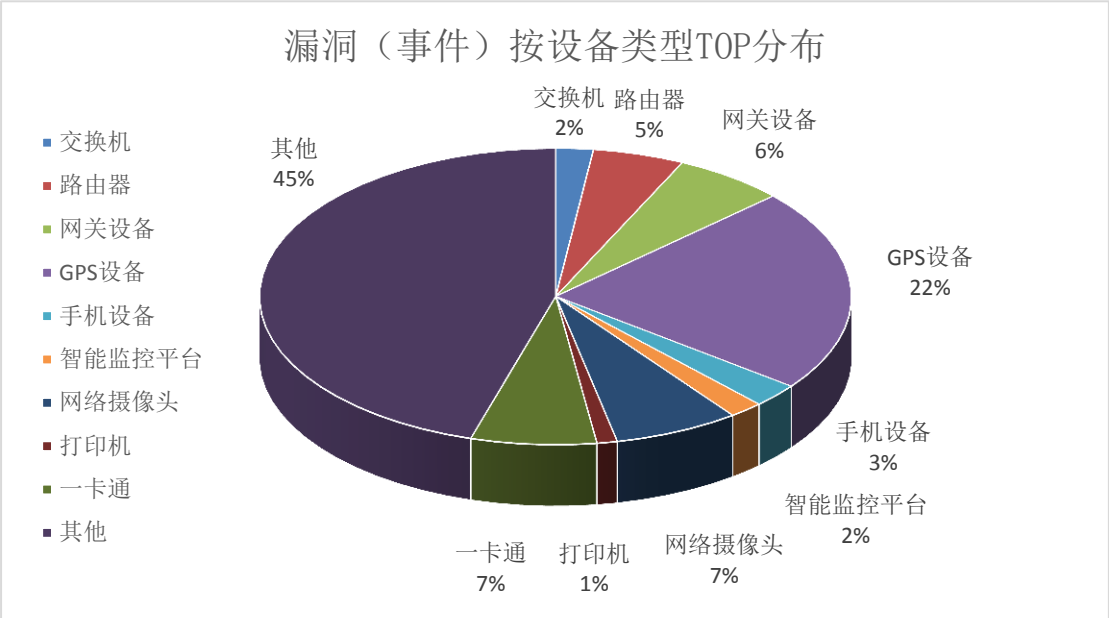

图 4 漏洞（通用）按设备类型TOP分布

五、传统网络设备漏洞收录统计

根据CNVD平台近五年公开发布的网络设备（含路由器、交换机、防火墙以及传统网络设备网关等产品）漏洞数量分布分析，传统网络设备漏洞数量总体呈上升趋势。2016年CNVD公开发布的网络设备漏洞697条，与去年环比增加27%。

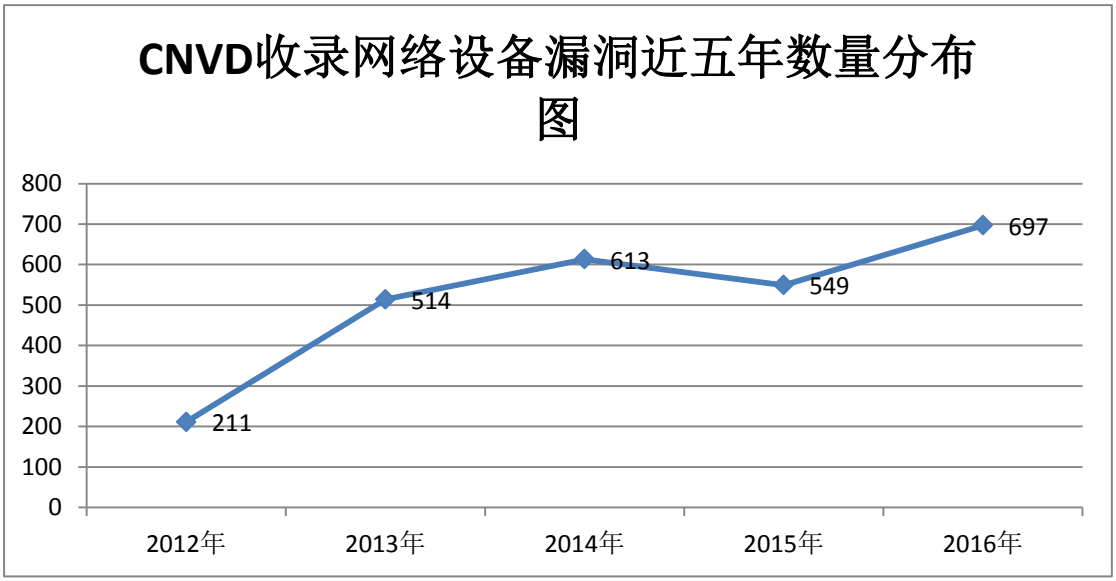

图5CNVD收录网络设备漏洞近五年数量分布

附：CNVD 2016年收录的典型IOT设备漏洞案例

- Fortigate防火墙存在SSH认证“后门”漏洞（CNVD-2016-00170）

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-00170

FortiGate(飞塔防火墙)是Fortinet（飞塔）公司推出的网络防火墙产品，用于防御网络层和内容层的网络和恶意代码等攻击。根据境外研究者的分析以及相关验证情况，业内认定FortiGate防火墙存在一处“后门”漏洞，漏洞形成的原因是由于FortiGate防火墙Fortimanager_Access用户的密码采用较为简单的算法来生成,攻击者通过分析破解后可直接获得认证的最高权限（root）权限，进而控制防火墙设备，后续攻击者可通过防火墙作为跳板，渗透内部区域网络，进行信息嗅探、数据拦截等操作。CNVD对该漏洞的综合评级为“高危”。

- Cisco ASA Software IKE密钥交换协议缓冲区溢出漏洞

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-00929

Cisco ASA是一款自适应安全设备，可提供安全和VPN服务的模块化平台，可提供防火墙、IPS、anti-X和VPN服务。由于Cisco ASA Software分段协议中的IKE网络密钥交换算法存在设计缺陷，IKEv1及IKEv2代码中存在缓冲区溢出漏洞。未经身份验证的远程攻击者利用漏洞发送特制的UDP数据包到受影响系统，可致设备重载或远程代码执行，进而可获取到目标系统的完整控制权。CNVD对该漏洞的综合评级为“高危”。

- Pulse Secure Desktop Client (Juniper Junos Pulse) 权限提升漏洞

http://www.cnvd.org.cn/flaw/show/CNVD-2016-05257

Pulse Secure Desktop Client（原用名为Juniper Junos Pulse）是访问Juniper Pulse Secure 网关的终端设备的客户端程序软件，Pulse Secure Desktop Client安装的系统服务dsAccessService.exe会创建一个名为NeoterisSetupService的命名管道。该命名管道的访问控制列表被设置为Everyone完全控制，所有用户均具有读写权限。管道服务端使用了自定义的加密算法，该管道用于安装新的系统服务时，可以作为自动升级机制的一部分。当有新数据写入管道时，这段数据会被当作文件路径解密，指向的文件会被复制到C:\Windows\Temp\并执行。服务安装逻辑在dsInstallService.dll中实现，它首先读入路径并从路径中切出文件名。这个实现逻辑存在一个漏洞：只切出了路径中“\”字符之后的部分，但忽略了“/”字符。攻击者可以传入一个恶意构造的路径，再通过DLL劫持的方式即可实现权限提升和任意代码执行。CNVD对该漏洞的综合评级为“高危”。

- 网件Netgear多款路由器存在任意命令注入漏洞

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-12093

Netgear R7000、R6400和R8000是美国网件（Netgear）公司的无线路由器产品。Netgear上述路由器的固件包含一个任意命令注入漏洞。远程攻击者可能诱使用户访问精心构建的web站点或诱使用户点击设置好的URL，从而以设备root用户权限在受影响的路由器上执行任意命令。CNVD对该漏洞的技术评级为“高危”。

- 多款Sony网络摄像头产品存在后门账号风险

http://www.cnvd.org.cn/flaw/show/CNVD-2016-11973

Sony公司IPELA ENGINE IP系列摄像头产品包含多个产品型号，其中以SNC-*编号的摄像头原固件中，web版管理控制台包含两个经过硬编码且永久开启的账号，分别是用户名debug/密码popeyeConnection及用户名primana/密码primana，后者可用来开启Telnet访问，甚至可获取摄像头管理员权限。远程攻击者利用漏洞可使用Telnet/SSH服务进行远程管理，从而获得摄像头产品的完全控制权。CNVD对该漏洞的技术评级为“高危”。

- Android MediaTek GPS驱动提权漏洞

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-04723

Android on Android One是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套运行于Android One（智能手机）中并以Linux为基础的开源操作系统。MediaTek GPS driver是使用在其中的一个联发科（MediaTek）公司开发的GPS驱动组件。Android One设备上的Android 2016-07-05之前版本中的MediaTek GPS驱动存在提权漏洞。攻击者可利用该漏洞借助特制的应用程序获取特权。CNVD对该漏洞的技术评级为“高危”。

- 多款mtk平台手机广升FOTA服务存在system权限提升漏洞（魅魔漏洞）

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-11347

上海广升信息技术股份有限公司是全球领先的终端管理云平台提供商，FOTA（无线升级）为IoT设备（智能汽车、穿戴、家居、

VR等）提供专业的无线升级解决方案。多款mtk平台手机广升FOTA服务存在system权限提升漏洞。由于使用广升FOTA服务的手机存在某绑定服务的系统app存在漏洞，可达到以system权限执行命令。攻击者利用漏洞可将权限提升至system权限。CNVD对该漏洞的综合评级为“中危”。

- 格尔安全认证网关系统存在多处命令执行漏洞

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-09983

  格尔安全认证网关为网络应用提供基于数字证书的高强度身份认证服务和高强度数据链路加密服务。格尔安全认证网关系统存在多处命令执行漏洞。攻击者利用漏洞可构造请求，执行任意命令，写入webshell，获取服务器权限，构成敏感信息泄露。CNVD对该漏洞的综合评级为“高危”。

- Android NVIDIA摄像头驱动程序权限获取漏洞

  http://www.cnvd.org.cn/flaw/show/CNVD-2016-09382

  Android on Nexus 9是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套运行于Nexus 9（平板电脑）中并以Linux为基础的开源操作系统。NVIDIA camera driver是使用在其中的一个摄像头驱动程序。基于Nexus 9设备上的Android 2016-10-05之前的版本中的NVIDIA摄像头驱动程序存在权限获取漏洞。攻击者可借助特制的应用程序利用该漏洞获取权限。CNVD对该漏洞的综合评级为“高危”。

- Lexmark打印机竞争条件漏洞

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00801

Lexmark printer是美国利盟公司的一款打印机产品。Lexmark打印机的初始化进程中存在竞争条件漏洞。远程攻击者通过security-jumper状态的不正确检测绕过身份验证。CNVD对该漏洞的综合评级为“高危”。