网络打印机安全研究与防护建议

Research and protection proposal for network printer security

李莉，陈诗洋，杨子羿，付凯
（中国信息通信研究院，北京 100191）

摘要：随着物联网技术与协同办公技术的不断发展，越来越多的网络打印机被应用到公司、政府部门、医院、学校等单位和机构。由于其功能单一性，我们往往忽略其安全性。然而打印设备往往部署在内部网络，通过它们可直接访问内部敏感信息。因此打印机网络安全不容忽视。近年来，打印机安全逐渐被安全界所关注，有关网络打印机的安全事件日益增多。本文主要介绍网络打印机存在的安全风险以及常见的攻击方法，并提出相应的防护建议。

关键词：打印机；安全；网络安全

0 引言

网络打印机是传统打印机和互联网应用的结合，网络打印设备完美的解决了办公中存在的互联共用问题，满足了企业的办公需求。但因其功能单一，其安全性不如交换机路由器等其他网络设备一样受到重视，导致网络打印机存在诸多安全隐患。而且由于打印设备往往部署在内部网络，黑客们可以其为跳板，对内网进行一系列攻击。近年来，有关网络打印机的漏洞披露和攻击事件日益增多。

2012年11月，美国计算机应急响应小组（CERT）发布网络预警称，三星的打印机（目前看来是所有版本）中存在漏洞，允许攻击者完全控制设备[1]。2013年1月，JetDirect（惠普打印软件）被Guerrero（西班牙研究人员）发现存在漏洞，允许入侵者对存在漏洞的网络打印机进行攻击，造成打印机拒绝服务状态，部分打印文档还可以被入侵者直接访问，而无需通过安全防护[2]。2016年3月，Andrew Auernheimer（代号为“Weev”，此前为Goatse安全团队成员的知名黑客）在其博客上承认其入侵了上千台网络打印机，并使其打印出带有种族主义及反犹太人等信息的内容[3]。2016年9月，德国鲁尔大学的安全研究人员对多种品牌型号的网络打印机开展了一项深入的安全研究。他们通过对20种不同品牌型号的打印机进行测试后发现，每一种品牌的打印机都存在不同程度的攻击可能性和漏洞[5]。另外，他们还给出了测试过程中使用的打印机入侵利用工具：PRinter Exploitation Toolkit(PRET)[4]。2017年2月，国外有一个自称“stackoverflowin”的黑客入侵了超过15万台打印机。被入侵的这些打印机全部都打印出了这名黑客留下的警告信息[6]。

此外，我们根据CVE（Common Vulnerabilities and Exposures，http://cve.mitre.org/）的数据如表1，分析得到各品牌打印机在1999年至2016年期间披露的各类型漏洞。

由以上披露的漏洞以及安全事件可以看出，网络打印机安全现状不容乐观。但由于打印机的特殊性，人们往往不重视其安全性。据中国电信股份有限公司北京研究院与北京神州绿盟信息安全科技股份有限公司联合发布的《2017年物联网安全研究报告》[7]可知，全球暴露在互联网上的打印机数量高达898173台，其中国内打印机的暴露数量就高达63495台。而且需要注意的是，

表1 近年来各品牌打印机CVE数量

品牌	Xerox	HP	Canon	Lexmark	Brother	Kyocera	Oki	Toshiba	其他
CVE数量	52	40	8	8	5	3	2	2	5

表2 网络打印机风险技术类型漏洞分布情况

漏洞类型	CVE数量
恶意PostScript打印任务（Malicious PostScript print jobs）	6
恶意PJL打印任务（Malicious PJL print jobs）	3
恶意处方打印任务（Malicious PRESCRIBE print jobs）	1
固件或软件更新（Firmware or software updates）	3
恶意IP数据包（Specially crafted IP packets）	3
网络服务（Network services）	23
Web应用（Web application）	63
未知或内部错误（Unspecified or internal vectors）	19
物理接触（Physical access to device）	4

报告中所列的打印机设备数量只是通过网络空间搜索引擎识别出的结果，很多打印机设备暴露出来的端口特征不明显，因此实际暴露的设备可能远远大于统计结果。暴露在互联网上的打印机设备不一定存在安全问题，但存在被攻击利用的风险。假如这些网络打印机设备被恶意地利用，很有可能就形成一个类似于Mirai的僵尸网络，后果不堪设想。因此，网络打印机的安全问题应受到用户与厂商的高度重视。为了提高人们对网络打印机安全的认识，下面我们将介绍网络打印机现有的安全隐患，常见的攻击方式，并提出相应的防护措施。

1 网络打印机面临的安全风险

基于德国鲁尔大学Jens Müller等人的研究成果[5]与对网络打印机CVE统计数据的分析，我们主要从攻击者类型、漏洞类型以及攻击手段来介绍网络打印机所面临的安全风险。

网络打印机的潜在攻击者主要可分为3种。第一种为内部攻击者，此类攻击者可以在打印机所在内部网络潜伏，直接执行物理攻击。主要攻击手段如下。

（1）通过USB外联设备或者内存卡把攻击程序插入到内部网络；

（2）直接连接目标打印机，比如通过USB外联设备等方式。

（3）更改打印机设置或者操作关键键位，譬如恢复出厂设置等。

第二种为网络攻击者，该攻击者可以远程攻击目标打印机，主要攻击方法如下。

（1）对打印机开启的端口打印服务攻击如：SMB、FTP、9100、Web、LPD、IPP或SNMP等。

（2）将后门植入到目标，以备长期的攻击。

第三种为浏览器攻击者，主要的攻击手段如下。

（1）利用钓鱼邮件等方式攻击目标网络内的工作人员。

（2）通过网络打印机存在的漏铜，如XSS等，将恶意打印脚本注入到打印机。

（3）渗透进入内网，对打印机间接控制。

基于对已公布的网络打印机漏洞数据整理分析，我们发现网络打印机的漏洞主要集中在Web应用（如存在XSS漏洞，CSRF漏洞等）、网络服务（FTP，Telnet等）与未知或内部错误。表2列出了网络打印机漏洞按风险技术类型分布情况，其中PostScript是一种与设备无关的打印机语言，PJL则是打印机作业语言。

此外，针对近期爆出的打印机安全事件，我们总结出几种现实中已经实现的攻击手段。

（1）Dos攻击（拒绝服务攻击）：攻击者可通过几行简单的PostScript代码，就可实现对打印机的DoS攻击，让打印机执行一个无限循环任务，直到资源耗尽。

（2）打印任务控制：由于一些PDL语言（打印机页面描述语言）支持任意修改操作，所以攻击者可以进行一系列恶意攻击，如打印内容覆盖，打印内容置换等。此外如果打印机使用PostScript命令，攻击者可以通过其获取打印任务，进而获取敏感信息。

（3）信息泄露攻击：打印机9100端口打印服务支持双向通道，因此可导致打印机某些敏感信息泄露。此外攻击者还可通过访问打印内存获取敏感信息，譬如攻击者可通过入侵打印机后访问内存和文件系获取密码。

（4）远程代码执行攻击（RCE）：由于某些品牌打印机存在缓冲区溢出漏洞，如HP系列部分激光打印

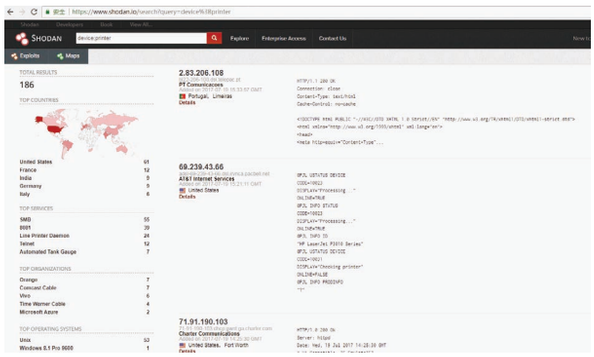

图1 shodan搜索公网上的打印机

图2 存在弱口令的网络打印机

机中存在的LPD协议缓冲区溢出漏洞，攻击者可精心构造数据包，使网络打印机执行恶意代码。此外，攻击者还可以通过构造虚假固件或软件升级包令打印机执行恶意代码。

（5）跨站打印（Cross-site printing，XSP）攻击：攻击者可通过CORS spoofing（跨源资源共享欺骗）利用Web进行XSP攻击。

此外，一个很常见且最容易实现的攻击方法为弱口令攻击。大多数打印机都设置有初始密码，但是人们往往未更改此密码。攻击者可通过shodan（https://www.shodan.io/）、钟馗之眼（http://www.zoomeye.org/）等网络空间搜索引擎搜到暴露到公网上的打印机，尝试进行弱口令暴力破解攻击，从而获取最高管理员权限。更有甚者，很多暴露在互联网上的网络打印机HTTP服务没有启用认证机制，这就意味着远程攻击者不需要登录即可进入打印机管理界面。下面我们给出一个弱口令攻击实例。图1是通过shodan搜索公网上的打印机，而图2则是搜索到的一个存在弱口令的打印机。我们只需输入该打印机设备出厂默认密码就可以直接得到目标打印机Admin管理员权限，进而可以进行查看打印信息、控制打印任务等恶意行为。

另外，我们还可通过德国鲁尔大学研究员开发的打印机入侵利用工具PRinter Exploitation Toolkit[6]对打印机进行测试与攻击。该工具基于python实现，大大简化终端攻击者与目标打印机之间的通信交流。此外，该工具可自动化搜寻局域网内的网络打印机，实现自动化攻击。

最后为验证PRinter Exploitation Toolkit工具的有效性，我们基于实验室网络打印机设备搭建环境进行攻击测试实验。实验中共使用两台打印机设备，型号分别为HP Color LaserJet CP2025dn与RICON MP 5054。实验过程可分为简单两步：首先将打印机设备与测试PC连接到同一个局域网内；然后在测试PC上使用PRinter Exploitation Toolkit工具，进行攻击测试。攻击命令如下：./pret.py 打印机IP地址 打印机所使用语言（PS、PJL、PCL），攻击效果见图3与图4。从图中，我们可以看到，攻击者未经允许即可连接到网络打印机并可轻易获取打印机型号、版本以及执行shell命令等危险行为。

2 防护建议

由《2017年物联网安全研究报告》[7]可知，只有不到44%的IT经理人把打印机列入了安全策略，与此同时，也仅有不到50%的使用者会使用打印机的“管理密码”功能，这意味着全球数以亿计的商务打印机中只有不到2%的打印机是真正安全的。为减少网络安全打印机被攻击风险，我们从安全配置以及漏洞防御角度针对2中总结的网络打印机存在的安全风险与攻击手段提出以下几点防护建议。

（1）及时更改初始默认密码，并及时删除多余和过期的账户。若使用默认账户密码，则可能受到未经授权的用户访问，个人数据和机密信息就有可能被更改或窃取。

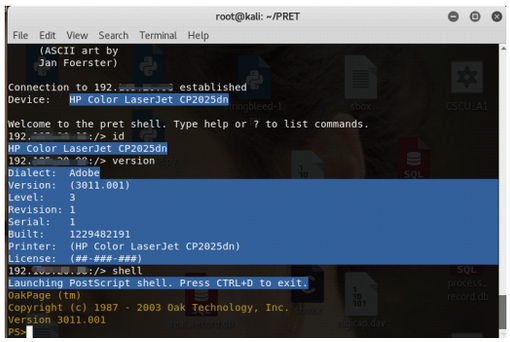

图3 PRET工具攻击效果图1

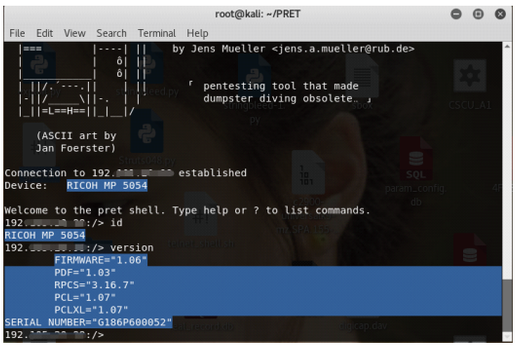

图4 PRET工具攻击效果图2

（2）将打印机安装 在设有防火墙、无线路由器或其他非直连网络方式保护的网络上，并建议采用私有IP地址以及互联网防火墙安全策略，对相应的网络协议和端口进行可访问限制。若网络打印机直接暴露在公网上，将增大其被攻击的风险。

（3）遵循最小安装原则，关闭不必要的端口与服务，譬如Telnet、FTP等功能，禁用不必要的服务组件、应用插件等，减少被入侵的风险。

（4）做好物理隔离，避免未经授权的陌生人直接接触或使用网络打印机，减少其受到物理攻击的可能性。

（5）在远程维护管理时，要做好访问限制，限制用户登录IP及访问权限，防止用户访问配置文件等敏感文件。应使用具有加密协议的登录控制模块，如SSH、VPN等，同时要及时将多余和过期的远程维护账户删除。

（6）要长期的关注打印机的固件和软件的升级公告，并及时从官方网站下载相应的固件和软件的安装包，以防其他渠道的安装包被恶意篡改过，使得打印机遭受攻击。要做好漏洞补丁相关的维护工作，这样才能降低被攻击的风险。

（7）限制用户连接数量与任务数量，防止受到Dos攻击（拒绝服务攻击）。

（8）定期对打印机进行安全审计，应及时关注日志中的审计分析，对其中记录的攻击事件的危害性进行评估，并采取相应的措施来控制。

此外，对网络打印机管理员等相关人员进行安全相关培训，提高其安全意识，使其掌握基本的信息安全事件防范技能，尽量减少网络打印机被攻击的风险以及被攻击后所造成的损失。

3 结论

随着对支持移动设备打印的需求越来越大，支持Wi-Fi直连、NFC打印、云打印等移动功能的网络打印机逐渐成为人们日常生活办公中不可缺少的电子设备。学校、政府部门、医院等各个单位与机构都会使用打印机。通过shodan、钟馗之眼等网络空间搜索引擎简单搜到暴露到公网上的打印机就高达898173台。从安全的角度来看，由于打印设备部署于内部网络，通过它们可以直接访问到各种敏感信息，因此其安全性比较重要。但由于其功能特殊性，人们往往忽略其安全性，导致打印机安全问题颇多，引发的安全事件也逐渐增多。为提高人们对网络打印机安全的重视，本文着重介绍了打印机面临的主要安全风险，得出其现有安全现状不容乐观，并总结出常见的攻击方法，最后提出了相对应的防护建议。本文为以后的打印机安全研究提供了一定的参考。

参考文献

[1]Hihei.三星全系打印机发现严重漏洞[EB/OL].freebuf.(2012-11-28)[2018-05-14]. http://www.freebuf.com/news/6330.html.
[2]Cs24:惠普打印软件JetDirect漏洞致多款网络打印机受威胁[EB/OL].freebuf.(2013-01-29)[2018-05-14]. http://www.freebuf.com/articles/system/7115.html.
[3]寰者.这名黑客的四行代码让数千台打印机宣传种族主义[EB/OL].freebuf.(2016-03-30)[2018-05-14]. http://www.freebuf.com/articles/web/100255.html.
[4]Bimeover.15万台打印机被黑，打印出了一堆奇怪的东西[EB/OL].freebuf.(2017-02-09)[2018-05-14]. http://www.freebuf.com/news/126336.html.
[5]M ü ller J,Mladenov V,Somorovsky J,et al.SoK: Exploiting Network Printers[J/OL].2017 IEEE Symposium on Security and Privacy:213-230.(2017-05-22)[2018-05-14]. https://www.ieee-security.org/TC/SP2017/papers/64.pdf.
[6]Jensvoid, jurajsomorovsky, AnthonyMastrean, mladevbb: PRET[DB/OL].GitHub.(2017-04-24)[2018-05-14]. https://github.com/RUB-NDS/PRET.
[7]薄明霞,唐洪玉,张星,等.2017物联网安全研究报告[EB/OL].(2017-12-12)[2018-05-14]. http://www.nsfocus.com.cn/content/details_62_2646.html

作者简介

李莉，工程师，主要研究方向：网络设备安全研究工作。
陈诗洋，助理工程师，主要研究方向：互联网新技术新业务安全评估研究工作。
杨子羿，助理工程师，主要研究方向：战略管理研究与咨询工作。
付凯，助理工程师，主要研究方向：网络设备安全研究工作。