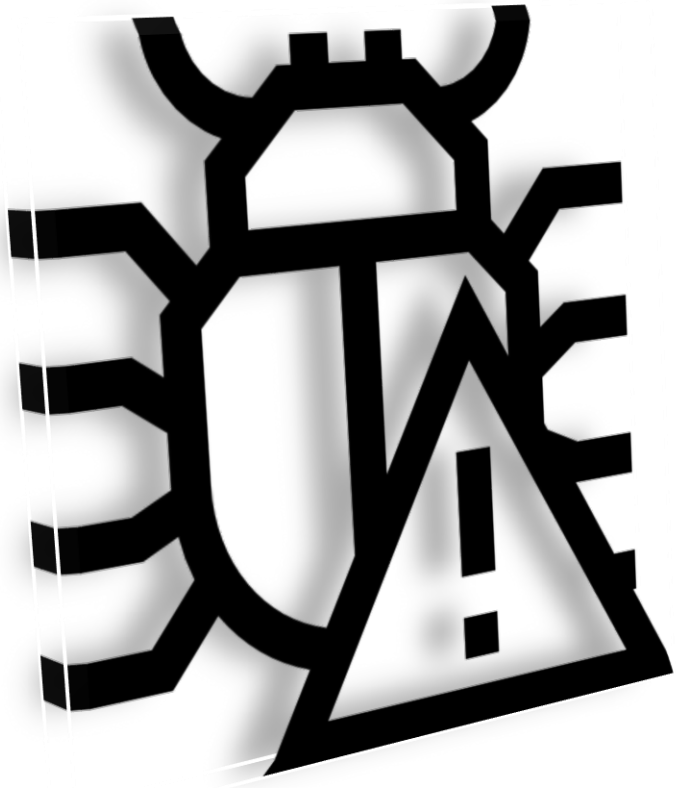
BUG REPORT



Generated by : Charchit Subedi

Date : 2022/march/30

Time : 3:39 pm

Website : https://www.uber.com/

Ip Address : 34.98.127.226

CONTENT

PG.NO

INTRODUCTION TO UBER COMPANY

In 2009, Uber was founded as Ubercab by Garrett Camp, a computer programmer and the co-founder of StumbleUpon, and Travis Kalanick, who sold his Red Swoosh startup for $19 million in 2007.

After Camp and his friends spent $800 hiring a private driver, he wanted to find a way to reduce the cost of direct transportation. He realized that sharing the cost with people could make it affordable, and his idea morphed into Uber. Kalanick joined Camp and gives him "full credit for the idea" of Uber.The prototype was built by Camp and his friends, Oscar Salazar and Conrad Whelan, with Kalanick as the "mega advisor" to the company.

DELAYED DISCLOSURE OF DATA BREACHES

On February 27, 2015, Uber admitted that it had suffered a data breach more than nine months prior. Names and license plate information from approximately 50,000 drivers were inadvertently disclosed.Uber discovered this leak in September 2014, but waited more than five months to notify the affected individuals.

An announcement in November 2017 revealed that in 2016, a separate data breach had disclosed the personal information of 600,000 drivers and 57 million customers. This data included names, email addresses, phone numbers, and drivers' license information. Hackers used employees' usernames and passwords that had been compromised in previous breaches (a "credential stuffing" method) to gain access to a private GitHub repository used by Uber's developers. The hackers located credentials for the company's Amazon Web Services datastore in the repository files, and were able to obtain access to the account records of users and drivers, as well as other data contained in over 100 Amazon S3 buckets. Uber paid a $100,000 ransom to the hackers on the promise they would delete the stolen data.Uber was subsequently criticized for

concealing this data breach.Khosrowshahi publicly apologized.In September 2018, in the largest multi-state settlement of a data breach, Uber paid $148 million to the Federal Trade Commission, admitted that its claim that internal access to consumers' personal information was closely monitored on an ongoing basis was false, and stated that it had failed to live up to its promise to provide reasonable security for consumer data. Also in November 2018, Uber's British divisions were fined £385,000 (reduced to £308,000) by the Information Commissioner's Office.

In 2020, the US Department of Justice announced criminal charges against former Chief Security Officer Joe Sullivan for obstruction of justice. The criminal complaint said Sullivan arranged, with Kalanick's knowledge, to pay a ransom for the 2016 breach as a "bug bounty" to conceal its true nature, and for the hackers to falsify non-disclosure agreements to say they had not obtained any data.

INTRODUCTION TO PJL

The Printer Job Language (PJL) was originally introduced by HP but soon became a de facto standard for print job control. ‘PJL resides above other printer languages’ and can be used to change settings like paper tray or size. It must however be pointed out that PJL is not limited to the current print job as some settings can be made permanent. PJL can also be used to change the printer's display or read/write files on the device. There are many dialects as vendors tend to support only a subset of the commands listed in the PJL reference and instead prefer to add proprietary ones. PJL is further used to set the file format of the actual print data to follow. Without such explicit language switching, the printer has to identify the page description language based on magic numbers.

INTRODUCTION TO NMAP

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

USE OF NMAP IN SCANNING

```
Applications  Places  Terminal                    Mar 30  2:51 PM
                                saugat@kali: ~/Desktop/PRET
saugat@kali: ~/Desktop/PRET                      saugat@kali:
┌──(saugat💔😈kali)-[~/Desktop/PRET]
└─$ sudo nmap -O --script vuln --script firewall-bypass uber.com
[sudo] password for saugat:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 14:27 +0545
Stats: 0:06:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.70% done; ETC: 14:33 (0:00:01 remaining)
Stats: 0:13:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 14:40 (0:00:00 remaining)
Stats: 0:18:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 14:45 (0:00:00 remaining)
Nmap scan report for uber.com (34.98.127.226)
Host is up (0.044s latency).
rDNS record for 34.98.127.226: 226.127.98.34.bc.googleusercontent.com
Not shown: 963 filtered tcp ports (no-response)
PORT      STATE SERVICE
43/tcp    open  whois
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
```

```
8085/tcp  open  unknown
8086/tcp  open  d-s-n
8088/tcp  open  radan-http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
8089/tcp  open  unknown
8090/tcp  open  opsmessaging
8099/tcp  open  unknown
9100/tcp  open  jetdirect
9200/tcp  open  wap-wsp
20000/tcp open  dnp
30000/tcp open  ndmps
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (86%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1246.49 seconds

┌──(saugat💔😈kali)-[~/Desktop/PRET]
└─$
```

In the Above screenshot We have scanned the host **https://www.uber.com/** using Nmap Tool . We have found that jetdirect is open at port 9100 .

So, Let's try to Find the Vulnerability using google

Applications Places Google Chrome Mar 30 4:58 PM

9100/tcp open jetdirect - Goo

google.com/search?q=9100%2Ftcp+open+jetdirect&oq=9100%2Ftcp+open+jetdirect&aqs=chrome..69i57j69i60l2.19745j0j...

Maps Gmail YouTube Facebook Private... Meet - ktz-cmcp-... Hack The Box :: H... New Tab Web Slice Gallery

Google

9100/tcp open jetdirect

All Images Videos Maps More Tools

About 262,000 results (0.39 seconds)

https://book.hacktricks.xyz › pentesting › 9100-pjl

9100 - Pentesting Raw Printing (JetDirect, AppSocket, PDL ...

Raw port 9100 printing, also referred to as JetDirect, AppSocket or PDL-datastream actually is not a printing protocol by itself ... **9100/tcp open jetdirect**.

You've visited this page 4 times. Last visit: 3/30/22

People also search for

jetdirect port 9100 exploit github | port 9100 used for
jetdirect telnet exploit | port 515 printer exploit
9100 printing | tcp 9100

People also ask

How do I open port 9100?

What is the use of port number 9100?

What ports need to be open for printers?

Applications Places Google Chrome Mar 30 4:58 PM

9100 - Pentesting Raw Printin

book.hacktricks.xyz/pentesting/9100-pjl

Maps Gmail YouTube Facebook Private... Meet - ktz-cmcp-... Hack The Box :: H... New Tab Web Slice Gallery MyWay

HackTricks

- HackTricks
- About the author
- Getting Started in Hacking
- Pentesting Methodology
- External Recon Methodology
- Phishing Methodology
- Brute Force - CheatSheet
- Exfiltration
- Tunneling and Port Forwarding
- Search Exploits

SHELLS

Shells (Linux, Windows,

Powered By GitBook

9100 - Pentesting Raw Printing (JetDirect, AppSocket, PDL-datastream)

Basic Information

Raw printing is what we define as the process of making a connection to port 9100/tcp of a network printer. It is the default method used by CUPS and the Windows printing architecture to communicate with network printers as it is considered as '*the simplest, fastest, and generally the most reliable network protocol used for printers*'. Raw port 9100 printing, also referred to as JetDirect, AppSocket or PDL-datastream actually **is not a printing protocol by itself**. Instead **all data sent is directly processed by the printing device**, just like a parallel connection over TCP. In contrast to LPD, IPP and SMB, this can send direct feedback to the client, including status and error messages. Such a **bidirectional channel** gives us direct **access** to **results** of **PJL**, **PostScript** or **PCL** commands. Therefore raw port 9100 printing – which is supported by almost any network printer – is used as the channel for security analysis with PRET and PFT. (From here)

If you want to learn more about **hacking printers read this page**.

Default port: 9100

We can see that Jetdirect is the vulnerabity of the Printer. We can Try to Exploit the vulnerabity .

IMPACT OF JETDIRECT VULNERABITY

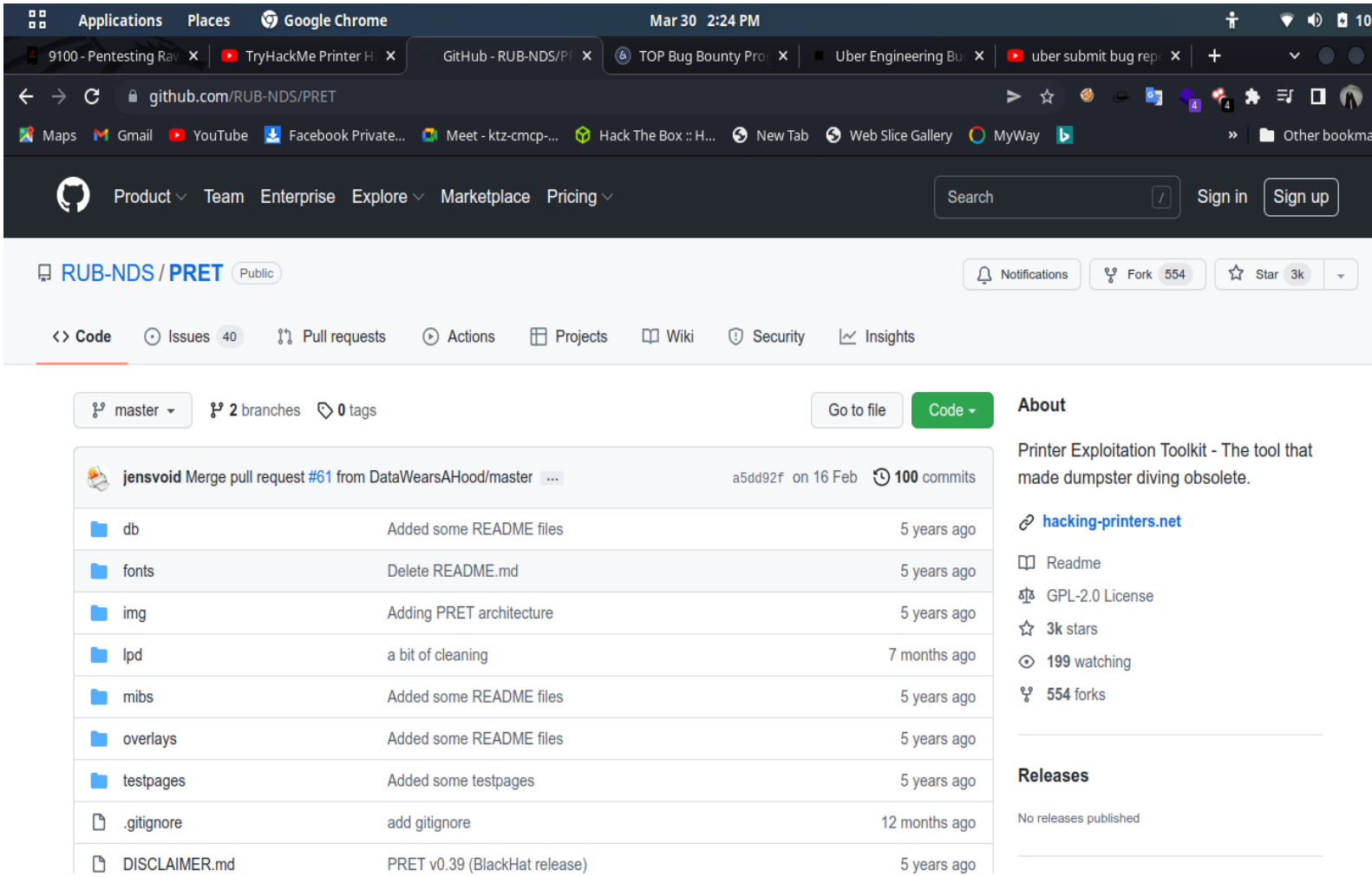
Various channels like USB, LPD, IPP, SMB, or raw port 9100 printing can be used as carriers to deploy malicious print jobs. While it is possible the attack printing protocols themselves, most attacks discussed in this wiki are targeted for the PostScript and PJL interpreters. The payload is just routed by any of the printing channels. This is important to note because it means whenever the attacker can somehow ‘print’ she can attack and exploit those interpreters. An attacker may use this flaw to gain administrative access on that printer.

An (wired or wireless) attacker connecting through a TCP/IP network can deploy print jobs over LPD, IPP, port 9100/tcp, FTP, SMB and the embedded web server. Under the assumption that no strong user authentication like smart card based access control or SSL client certificates is enforced, both attacker models do obviously have a channel to print which is the precondition for further attacks to be carried out. Both are certainly quite strong attacker models because they require direct access – either physical or logical – to the device. However, in penetration testing scenarios where sneaking into the building is not an option and the printer is not directly reachable over the internet, other deployment channels are required. In such cases, the victim's web browser can be used as a carrier for printer malware as discussed in cross-site printing.

POC

Let's try to exploit the vulnerability using "PRET" Tool which is easily available in the Github , The link for the tool is given below :

https://github.com/RUB-NDS/PRET



In the above screenshot the poc of tool is given.

```
Applications  Places  Terminal                                  Mar 30  3:04 PM
                                                saugat@kali: ~/Desktop/PRET
saugat@kali: ~/Desktop/PRET

┌──(saugat💔😈kali)-[~/Desktop/PRET]
└─$ python pret.py 34.98.127.226 pjl

      _______________
    _/______________/|
   /__________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===        |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |           |   ô| ||
  |___________|   ô| ||
  | ||/.´---.||    | ||      ⌜ pentesting tool that made
  |-||/____\||-.   | |´        dumpster diving obsolete··⌟
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 34.98.127.226 established
Device:   Receiving data failed (watchdog timeout)

Welcome to the pret shell. Type help or ? to list commands.
34.98.127.226:/> help

Available commands (type help <topic>):
=======================================
append  delete    edit    free  info    mkdir     printenv  set       unlock
cat     destroy   env     fuzz  load    nvram     put       site      version
cd      df        exit    get   lock    offline   pwd       status
chvol   disable   find    help  loop    open      reset     timeout
close   discover  flood   hold  ls      pagecount restart   touch
debug   display   format  id    mirror  print     selftest  traversal
```

The above screenshot is the main POC of Jetdirect Vulnerability . In the above screenshot I have run the “Pret” tool which I have downloaded from the Github .

I have write “ Python Pret.py < Ip address> pjl “ and the connection is established . When the connection is established I have got the prêt shell. Now I can completely executed the command showing from the help command.

SOLUTION FOR JETDIRECT VULNERABILITY

- Additional means of protection (does not address the SNMP vulnerability)
- Define a telnet password (do not keep it empty)
- Create an 'allow list' from the Telnet console to restrict access from defined IP-addresses

Vulnerabilities in SNMP Disclosure of HP JetDirect EWS Password is a high risk vulnerability that is also high frequency and high visibility. This is the most severe combination of security factors that exists and it is extremely important to find it on your network and fix it as soon as possible.

Reference : https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-disclosure-hp-jetdirect-ews-password.html