nathan31337 / Splunk-RCE-poc Public

Notifications Fork 25 Star 112

Code Issues 3 Pull requests Actions Projects Security Insights

main Go to file Code

nathan add blog post + bug was fixed earlier fde6e96 · last year 5 Commits

screenshots	:^)	last year
CVE-2023-46214.py	:^)	last year
README.md	add blog post + bug was fixed earlier	last year

About

No description, website, or topics provided.

- Readme
- Activity
- 112 stars
- 3 watching
- 25 forks

Report repository

Releases

No releases published

Packages

No packages published

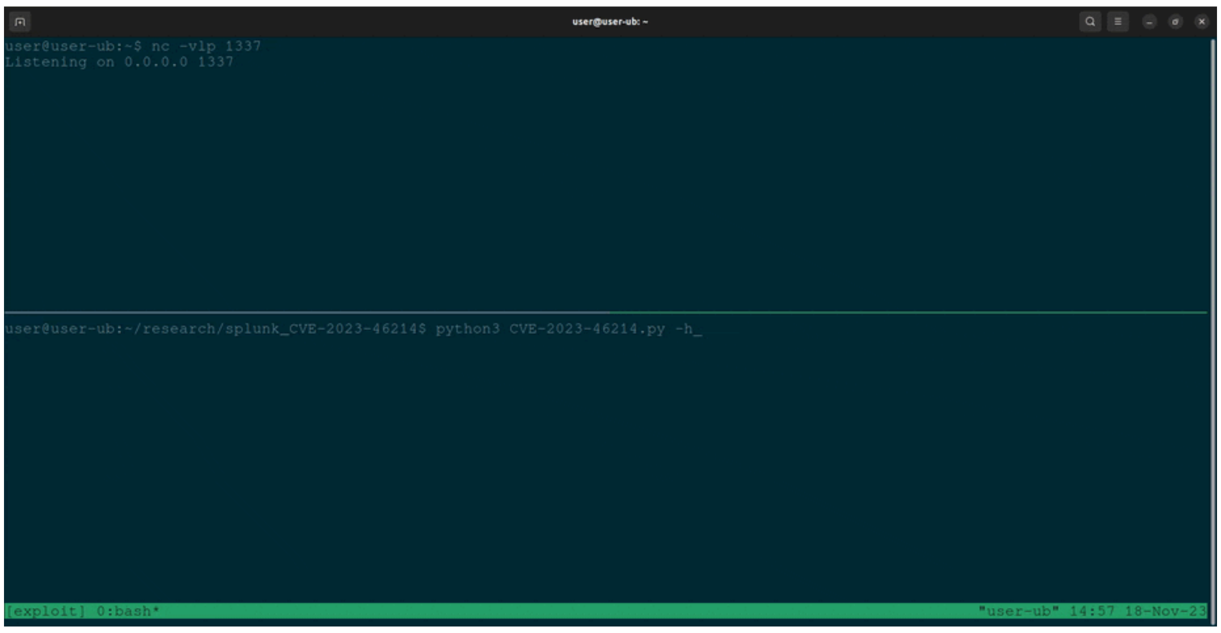
Languages

Python 100.0%

README

Splunk RCE - PoC

Proof of concept exploit for CVE-2023-46214, SVD-2023-1104



```
user@user-ub:~$ nc -vlp 1337
Listening on 0.0.0.0 1337
```

```
user@user-ub:~/research/splunk_CVE-2023-46214$ python3 CVE-2023-46214.py -h_
```

```
[exploit] 0:bash*                                                "user-ub" 14:57 18-Nov-23
```

Usage

The Splunk instance URL, username, password, reverse shell IP, and port are all required as command-line parameters. For example:

```
$ python3 CVE-2023-46214.py --url <Splunk_URL> --username <Username>
```

Prerequisites

- Splunk credentials with upload permission to adddatamethods
  - Note: another vector might be possible, this is just what I used
- Splunk is not running on SHC mode

Analysis

I've written a blog post detailing the methodology taken to uncover this vulnerability. If you are running into any issues with the script, the blog could be helpful as it details the manual steps for exploitation.

Analysis of CVE-2023-46214 + PoC

Legal Disclaimer

The Proof of Concept (PoC) script provided in this repository serves solely for educational and research objectives. Its purpose is to showcase a specific vulnerability and aid in comprehending associated security risks.

Any use of this script for unauthorized activities, including but not limited to unauthorized system access, unauthorized testing, or other forms of misuse, is unequivocally forbidden.

The creators and contributors of this repository disclaim all liability for the improper use or any damage or harm resulting from the use of this script. By utilizing this script, you consent to use it in a responsible manner and at your own risk.