CVE-2022-38301: Path Traversal in Onedev v7.4.14

Path Traversal in Onedev v7.4.14

CVE Number

CVE-2022-38301

Loginsoft ID

Loginsoft-2022-1010

Vulnerability Description

A path traversal vulnerability allows an attacker to gain unauthorized access to restricted directories and files on the server. An attacker with a project manager privilege can upload a malicious jar file into the “/opt/onedev/lib” directory as an artifact in project builds page which will be replacing the “io.onedev.server-plugin-executor-serverdocker-7.4.14.jar” file from the lib directory. Upon a server restart, the user can execute the uploaded malicious jar file by running a build which internally calls the executor plugin that leads to **Remote code execution.**

CWE ID

CWE-22

Versions Affected

<= v7.4.14

CVSS Score

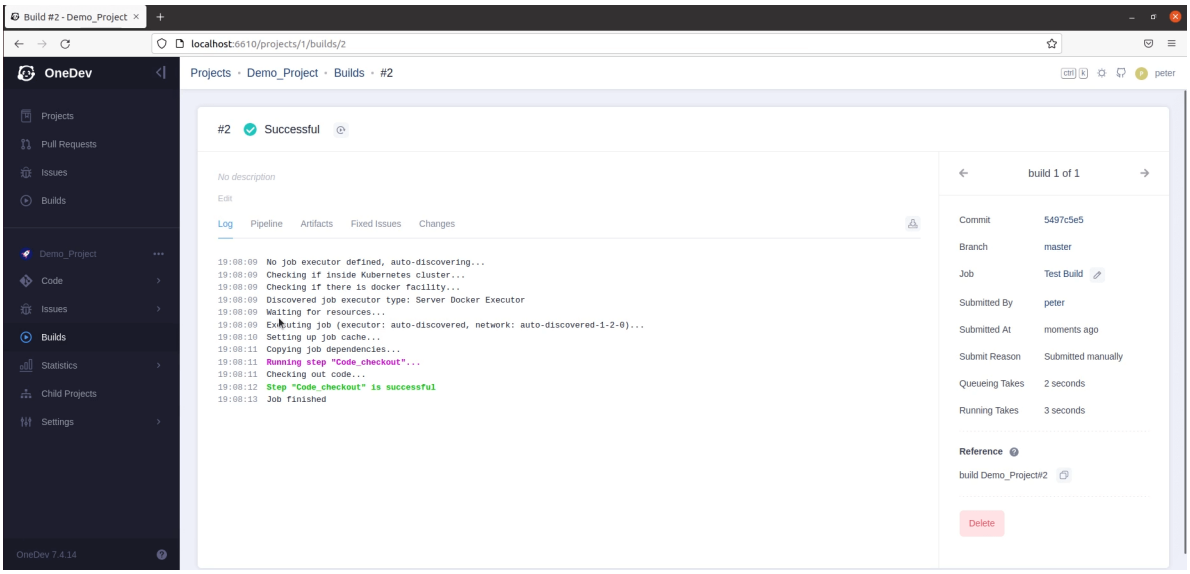
7.5 (High)

CVSS Vector

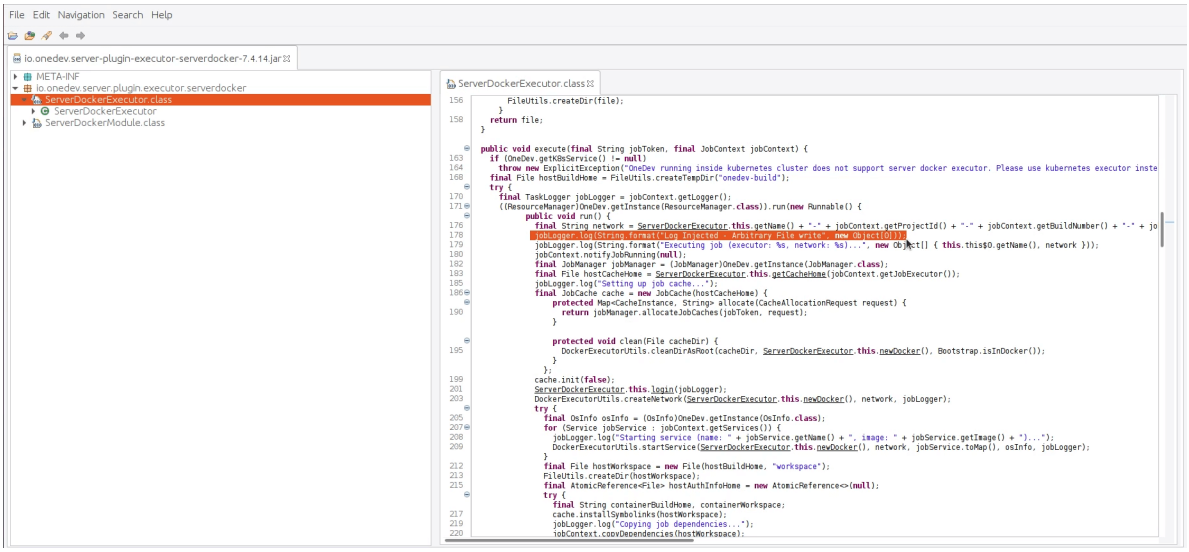
CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Steps to reproduce:

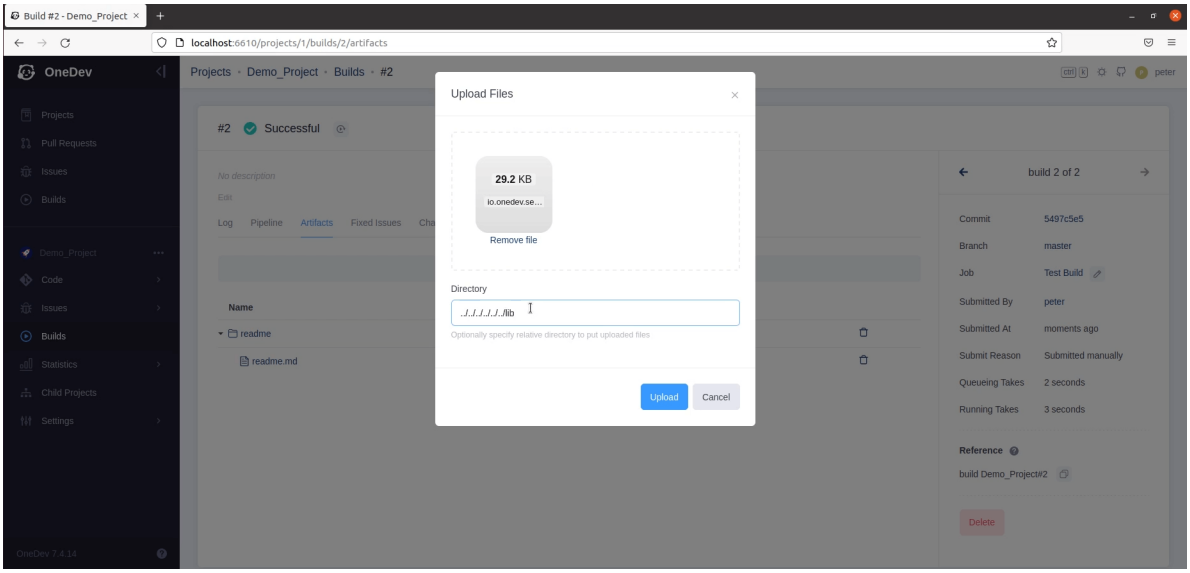
- Login into application as a user with project manager privilege
- Create and run any sample build with any executor



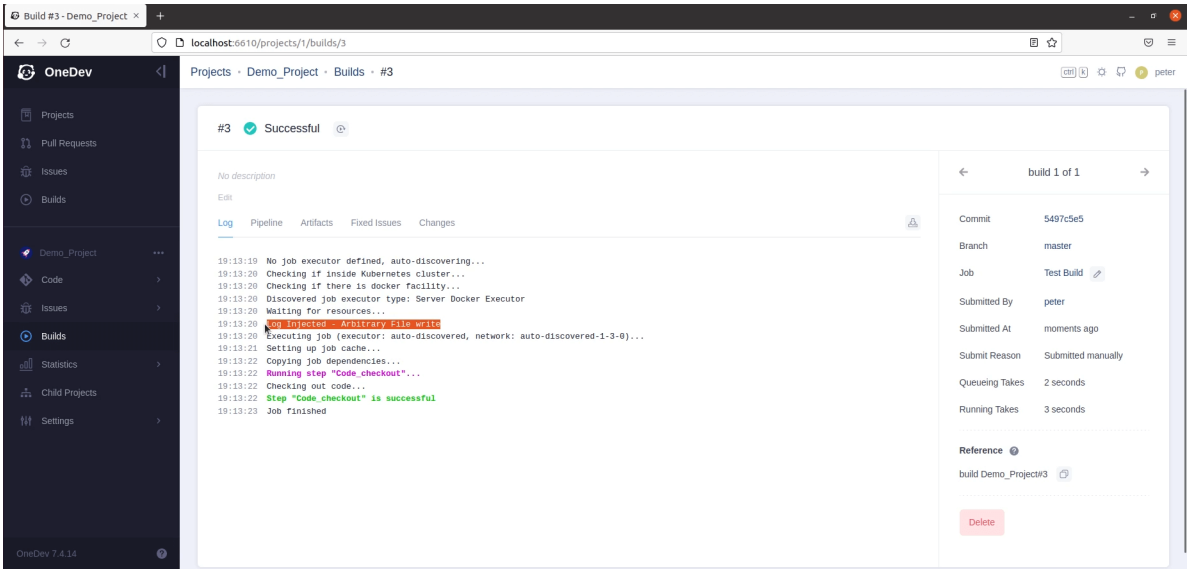
- Select any build and navigate to the artifacts upload page to create a sample folder and upload a file
- Create a jar file with malicious code and pack it with same file name as on the server



- Now upload the malicious jar file to the directory with payload “../../../../../../lib” which will replace the original jar file in the lib directory



- After restarting the server, access the application and run any build
- We can see the uploaded malicious jar file executes and inserted log is generated during the build execution



Impact

This vulnerability leads to arbitrary file write in server and can also inject malicious jars that leads to remote code execution.

To protect the application from this weakness it is advised to follow these instructions:

- Normalizing user-supplied input against such attacks as Path/Directory Traversal
- Do not allow special characters “..”,”/” in the file name or directory name

Fix Commit

https://github.com/theonedev/onedev/commit/5b6a19c1f7fe9c271acc4268bcd261a9a1cbb3ea

Identified Date

09 August, 2022

Disclosure Date

09 August, 2022

Credit

Bhargava Ram Koduru

Let us know how we can help you

CONTACT

soft

US Office
4437 Brookfield Corporate Drive, Suite 101
Chantilly, VA USA 20151.
+1 703 956 7410

Canada Office
7-7003 Steeles Ave W, Toronto,
ON M9W 0A2, Canada.

India Office
1-63-5-8B, Kavuri Hills, Jubilee Hills,
Hyderabad-500033.