Snyk Vulnerability Database › Go ›
github.com/valyala/fasthttp

Directory Traversal

Affecting github.com/valyala/fasthttp package, versions <1.34.0

INTRODUCED: 21 FEB 2022 CVE-2022-21221 ?
CWE-22 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `github.com/valyala/fasthttp` to version 1.34.0 or higher.

Overview

github.com/valyala/fasthttp is a fast HTTP server and client API.

Affected versions of this package are vulnerable to Directory Traversal via the `ServeFile` function, due to improper sanitization. It is possible to be exploited by using a backslash `%5c` character in the path.

Note: This security issue impacts Windows users only.

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.

Search by package nar

5.9
MEDIUM

Snyk CVSS

Attack Complexity	High	?
Confidentiality	HIGH	?

See more

› NVD 7.5 HIGH

`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
- GitHub Issue
- GitHub Release Notes
- GitHub "Warning" Commit

Snyk Learn

Learn about Directory Traversal vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-GOLANG-GITHUBCOMVALYALAFASTHT 2407866
Published	15 Mar 2022
Disclosed	21 Feb 2022
Credit	egovorukhin

Report a new vulnerability

Found a mistake?

Test with Github

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

DevSecCon

Join the >> community

Registered in England and Wales. Company number: 09677925

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