secoats dos in restify-paginate ... on Feb 25, 2021 History

| | |
|---|---|
| .. | |
| node_modules | last year |
| README.md | last year |
| minimal.js | last year |
| minimal_quickfix.js | last year |
| package-lock.json | last year |
| package.json | last year |
| proof_of_concept.py | last year |
| vulnserver.js | last year |

README.md

# CVE-2020-27543 - DoS in restify-paginate 0.0.5

Insufficient HTTP header validation in npm package **restify-paginate 0.0.5** can lead to a Denial-of-Service (DoS) attack.

When included, restify-paginate acts as a middleware and gets executed every time a HTTP request is made to an endpoint. Its purpose is splitting up large JSON responses into several pages.

The affected version 0.0.5 was released 3 years ago (2018) and has **2,183 weekly downloads** (npm, checked Feb. 2021) and **at least 150,000 total downloads** since release (npm-stat.com, checked Feb. 2021).

## Details

If the package is used as described in the npm README / Github README, then **any HTTP request without the HTTP Host-header sent to any existing API endpoint** will cause the server to crash due to an uncaught exception in the middleware. Any existing HTTP endpoint can be used to cause the crash, regardless of whether the pagination feature is actually used to construct the HTTP response.

Such an HTTP request could look like this:

```
GET / HTTP/1.0
User-Agent: Whatever
Connection: close
```

Note that the above request is a valid HTTP/1.0 request (Host header not required). But neither Node.js nor Restify will reject HTTP/1.1 requests with missing Host header either, even though the header is technically required (tested with Node.js v12.19.0 Windows 64; Restify 8.5.1).

If it was used, this exception would not get caught by the standard restify error handler "restify-errors" either (would normally send a 500 response code and resume) because this type of uncaught exception in middleware is currently not supported by the error handler. This assumes the middleware is integrated as described in the restify-paginate README via `server.use(paginate(server, ...))`.

## Reproduce

Assuming you have Node.js 12 or newer installed. Navigate into the directory with the vulnserver.js file. Install restify and the affected version of restify-paginate via npm and start the example server:

```
npm install restify@8.5.1
npm install restify-paginate@0.0.5

node .\vulnserver.js
```

You can run `python3 proof_of_concept.py` to verify that the server is vulnerable. Adjust the socket options and request path as needed. The Node.js instance should crash with an uncaught exception.

## Remedies

A quick fix for users of restify-paginate is setting `hostname: false` in the `paginate()` options. This hostname option is set to `true` by default.

Disabling that option appears to skip over the affected code segment.

```
options = {
    hostname: false     // Quick Fix: Skip over affected code segment
}

var server = restify.createServer({ name: 'My API' });
```

```
server.use(restify.plugins.queryParser());
server.use(paginate(server, options));
```

## Publication Timeline

- 18.11.2020 - CVE-2020-27543 was reserved for this vulnerability by the Mitre Corporation
- 25.11.2020 - Developer was informed about the vulnerability via email. A 90 days responsible disclosure deadline was set in the report
- 24.02.2021 - The 90 days responsible disclosure deadline expired