New issue

Jump to bottom

Removed a bug which could cause a crash in HeaderParser, and as consequence could potentially crash a web server based on it #22

Open

RolandHeinze wants to merge 5 commits into `mscdex:master` from `RolandHeinze:header-parser-bug`

RolandHeinze commented on Aug 5, 2021

Function `HeaderParser.prototype._parseHeader()` uses a variable `h`, which in edge cases is used before it is initialized. As a consequence the statement

```
this.header[h][this.header[h].length - 1] += lines[i];
```

would crash. This can happen if an attacker uses a manipulated multipart/form-data header with a header name that starts with ' ' or '\t'. I wrote a simple HTML file that is exactly doing this using the fetch() function:

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
</head>

<body onload="sectest()">
<button id="security">Security Check</button>
<script>
  function sectest() {
    const button_sectest = document.getElementById('security');
    button_sectest.onclick = send;
  }
  function send(event) {
    event.preventDefault();
    fetch('form-image', {
      method: 'POST',
```

```
      headers: {
        ['content-type']: 'multipart/form-data; boundary=----WebKitFormBoundaryoo6vortfDzBsDiro',
        ['content-length']: '145',
        host: '127.0.0.1:8000',
        connection: 'keep-alive',
      },
      body: '------WebKitFormBoundaryoo6vortfDzBsDiro\r\n Content-Disposition: form-data; name="bildb
    });
  }
</script>
</body>
</html>
```

I used such an HTML file, and was able to crash Dicer and also Busboy. In particular, it happens if one uses the example server code presented on the Dicer GitHub repository. I think that it is a severe bug which should be removed as soon as possible.

Therefore, I wrote this PR. It

- removes the mentioned bug;
- removes a bug in the HeaderParser constructor functions which computed a wrong value for the variable `end`;
- removes some unnecessary code in `HeaderParser.prototype._parseHeader()`;
- removes the variable `_realFinish` and all of it's occurances in `Dicer.js` as it is not necessary, increases the code size, and adds unwanted complexity;
- removes an unnecessary `else if` clause in the function `Dicer.prototype._oninfo()`;

RolandHeinze changed the title ~~Removed a bug which could cause a crash in HeaderParser, and as consequence could potentially crash a web server based on~~ Removed a bug which could cause a crash in HeaderParser, and as consequence could potentially crash a web server based on it on Aug 5, 2021

RolandHeinze mentioned this pull request on Aug 5, 2021

Security alert: Busboy can crash on manipulated multipart/form-data header names
mscdex/busboy#250

Closed

srosset81 mentioned this pull request on Aug 9, 2021

Erreur aléatoire quand on POST des fichiers dans un container LDP assemblee-virtuelle/semapps#834

Closed

RolandHeinze added 5 commits 16 months ago

- `removed bug caused by uninitialized variable h in function HeaderPars…` b7fca2e
- `removed unnecessary code in funvtion` dbf3bfa
- `the value of end was calculated incorrectly in` 6549a54
- `removed variable _realFinish in` cba4d3c
- `removed unnecessary else if clause in function Dicer.prototype._oninfo.` 8003224

RolandHeinze force-pushed the `header-parser-bug` branch from **10898ae** to **8003224** 16 months ago

Compare

Uzlopak mentioned this pull request on Nov 24, 2021

BusBoy replacement? fastify/fastify-multipart#297

Closed

2 tasks

kibertoad commented on Nov 28, 2021

@RolandHeinze Are you using dicer as a part of busboy or separately?
Context for the question - we have forked busboy within fastify organization in order to restart development on it, and our original plan was to just embed dicer in it. However, if there is demand for fixed dicer outside of busboy, we can also provide that as a separate dependency.

Uzlopak mentioned this pull request on Nov 29, 2021

Fix Malformed header bug fastify/busboy#34

Merged

4 tasks

maxpoulin64 added a commit to maxpoulin64/lounge that referenced this pull request on Dec 4, 2021

- `Switch busboy implementation to @fastify/busboy` ✓ 2c2dd1c

maxpoulin64 mentioned this pull request on Dec 4, 2021

Switch busboy implementation to `@fastify/busboy` thelounge/thelounge#4428

Merged

nathan-gilbert commented on May 20

Hi devs, I'm starting to get Snyk High Vulnerability alerts regarding Dicer for all versions: https://snyk.io/vuln/npm%3Adicer

Any way I can help get this PR across the line?

👍 3

mscdex commented on May 20 Owner

@nathan-gilbert If you're just parsing web forms (multipart or urlencoded), `busboy` would be a better choice.

`dicer` was originally created for use by `busboy`, but it no longer depends on it.

👍 1

nathan-gilbert commented on May 20

@mscdex I'm not using `dicer` directly, but many of my dependencies are so it would be a much larger refactor than simply switching `dicer` for `busboy`.

mscdex commented on May 20 Owner

@nathan-gilbert If the parent dependency is an older version of `busboy`, releasing a new version of `dicer` would not help as those old versions of `busboy` used exact versions for the `dicer` dependency and not version ranges.

nathan-gilbert commented on May 20

@mscdex Yep, you're right. I thought there were more than just `busboy` using `dicer` but it doesn't look like it. I think all I need to do is upgrade `busboy`.

Thanks, sorry for taking up some time here.

harshagarwal00 mentioned this pull request on May 23

Security Issues in dicer package firebase/firebase-admin-node#1512

Closed

nsandeepn commented on May 23

There is a Denial of Service (DoS) security flaw has been introduced in multer@1.4.4. The details are available in the Snyk report: https://security.snyk.io/vuln/SNYK-JS-DICER-2311764
There is no fix version available. So It is impacting other modules which dependent on the multer module. So we are looking for fix version for this as soon as possible.

mscdex commented on May 23 Owner

@nsandeepn `multer` just needs to upgrade to the latest version of `busboy`. For existing `multer` installations, there's nothing that can be done (see #22 (comment)).

wprk mentioned this pull request on May 24

CVE-2022-24434: High severity vulnerability found in all versions #28

Closed

Karlinator commented on May 26

FYI it looks like firebase/firebase-admin-node depends on `dicer` directly, but only for parsing responses from the Firebase API. Should be no real danger there, just annoying to have the security warning.

AnkurBansalSF commented on May 26 • edited

@Karlinator
npm audit report

dicer *
Severity: high
Crash in HeaderParser in dicer - GHSA-wm7h-9275-46v2
fix available via `npm audit fix --force`
Will install firebase-admin@7.0.0, which is a breaking change
node_modules/dicer
firebase-admin >=7.1.0
Depends on vulnerable versions of dicer
node_modules/firebase-admin

2 high severity vulnerabilities

👍 2

yurisim commented on May 26

For people getting this error in snyk, if it isn't already apparent from the comments above...

An older version of busboy used this version of dicer that is throwing this problem.

Multer really just needs to update their packages,
see
expressjs/multer#1095

👍 2

 **jitbasemartin** mentioned this pull request on May 26

Crash in HeaderParser in dicer - git hub security alert #30

Open

 **argon1025** mentioned this pull request on May 27

dicer 패키지 보안 업데이트 TIL-Log-lab/Tilog-server-node-v2#83

Closed

 **Kondamon** mentioned this pull request on May 27

Crash in HeaderParser in dicer firebase/firebase-admin-node#1729

Closed

 **jaydenseric** mentioned this pull request on May 27

Update the `busboy` dependency to v1 jaydenseric/graphql-upload#311

Closed

rudxde commented on May 27

> multer just needs to upgrade to the latest version of busboy. For existing multer installations, there's nothing that can be done (see #22 (comment)).

This is not as easy as said, since the change in to not use dice is part of the braking release v1.0.0, which drops the support of older node versions. Upgrading to this version in multer would also require multer to create a breaking change release. (See: expressjs/multer#1097)

Creating a fix in dicer would enable different users to use the `override` feature of npm to quick-fix the issue.

Also: if you don't plan to support dicer further, i think it would be beneficial to deprecate/archive this repo and add some infos, that users can find easily.

👍 12

colinhowe commented on May 27 • edited

If anyone wants to patch around this in a minimal way until all their other dependencies update then we used this patch in Dicer (0.2.5):

```
diff --git a/node_modules/dicer/lib/Dicer.js b/node_modules/dicer/lib/Dicer.js
index 246b3ea..611cbeb 100644
--- a/node_modules/dicer/lib/Dicer.js
+++ b/node_modules/dicer/lib/Dicer.js
@@ -124,7 +124,11 @@ Dicer.prototype.setBoundary = function(boundary) {
   var self = this;
   this._bparser = new StreamSearch('\r\n--' + boundary);
   this._bparser.on('info', function(isMatch, data, start, end) {
-    self._oninfo(isMatch, data, start, end);
+    try {
+     self._oninfo(isMatch, data, start, end);
+    } catch (e) {
+      self.emit('error', e)
+    }
   });
 };
```

This catches the error and emits it so that Express can properly fail the request and get back to processing other requests. Arguably, this would be a good change to see in Dicer regardless.

👍 13

mscdex mentioned this pull request on May 30

Vulnerability Fix #32

Closed

hairmare mentioned this pull request on May 31

Fix code scanning alert - CVE-2022-24434 wellenplan/wellenplan#6

Closed

1 task

lahirumaramba commented on Jun 1 • edited

We also have a direct dependency on `dicer` in firebase-admin-node. Fixing `dicer` would help developers who are currently have their releases blocked on `npm audit` (see firebase/firebase-admin-node#1718 (comment)). It will also provide a stopgap solution for package maintainers and buy some time to implement a proper fix (updating busboy etc.).

Also agree with **@rudxde** if you no longer recommend developers to use `dicer` directly, deprecating the module would help.

13 1

Kondamon commented on Jun 3

> `dicer` was originally created for use by `busboy`, but it no longer depends on it.

@mscdex: So, is dicer still going to be maintained? If no, does anything speak against marking dicer as deprecated?

mscdex commented on Jun 3 Owner

@Kondamon It's low priority at the moment. `dicer` really needs a rewrite, much like `busboy` had, because node streams have come a long way since I first wrote the modules.

1

hardysabs2 commented on Jun 7

Presumably indirect dependencies such as this...

apollo-server > apollo-server-core >
@apollographql/graphql-upload-8-fork > busboy > dicer

...are of very little security risk remaining on dicer v0.3.1 with no fix?

👍 1

rafaelmaeuer commented on Jun 7

> If anyone wants to patch around this in a minimal way until all their other dependencies update then we used this patch in Dicer:
>
> ```
> diff --git a/node_modules/dicer/lib/Dicer.js b/node_modules/dicer/lib/Dicer.js
> index 246b3ea..611cbeb 100644
> --- a/node_modules/dicer/lib/Dicer.js
> +++ b/node_modules/dicer/lib/Dicer.js
> @@ -124,7 +124,11 @@ Dicer.prototype.setBoundary = function(boundary) {
>    var self = this;
>    this._bparser = new StreamSearch('\r\n--' + boundary);
>    this._bparser.on('info', function(isMatch, data, start, end) {
> -    self._oninfo(isMatch, data, start, end);
> +    try {
> +     self._oninfo(isMatch, data, start, end);
> +    } catch (e) {
> +      self.emit('error', e)
> +    }
>    });
>  };
> ```
>
> This catches the error and emits it so that Express can properly fail the request and get back to processing other requests. Arguably, this would be a good change to see in Dicer regardless.

On which version of dicer did you create/apply this fix?

colinhowe commented on Jun 7

@rafaelmaeuer 0.2.5 - I'll update my comment to say that

mscdex mentioned this pull request on Jun 13

Denial Of Service (DoS) Vulnerability #34

Closed

 **CobyPear** mentioned this pull request on Jun 17

Clean up peer dependency warnings and latest audit pantheon-systems/decoupled-kit-js#148

Merged

herbola approved these changes on Jun 23

View changes

 **TheKingTermux** mentioned this pull request on Jun 23

Crash in HeaderParser in dicer TheKingTermux/alice#83

Open

4 tasks

 **wojtekmaj** mentioned this pull request on Jul 29

Security vulnerability due to dicer 0.2.5 expressjs/multer#1122

Open

 **github-actions** bot mentioned this pull request on Aug 1

CVE-2022-24434 - high detected in dicer['0.3.0'] rhicksiii91/goof#305

Open

vinutha93bnvs commented on Sep 12

> Presumably indirect dependencies such as this...
>
> apollo-server > apollo-server-core > @apollographql/graphql-upload-8-fork > busboy > dicer
>
> ...are of very little security risk remaining on dicer v0.3.1 with no fix?

@hardysabs2
Did you find a solution for this?

 **mpacary** mentioned this pull request on Oct 21

Potential crashes with "dicer" dependency mixmaxhq/batchelor#35

Open

Reviewers

herbola ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

16 participants