May 14, 2021

GHSL-2021-019: File disclosure in express-hbs - CVE-2021-32817

Agustin Gianni

Coordinated Disclosure Timeline

- 01/25/2021: Report sent to maintainer
- 01/28/2021: Maintainer acknowledged report
- 04/22/2021: Maintainer added documentation warning users of the dangers of the pattern

Executive Summary

The Express render API was designed to only pass in template data. By allowing template engine configuration options to be passed through the Express render API directly, downstream users of an Express template engine may inadvertently introduce insecure behavior into their applications with impacts ranging from Cross Site Scripting (XSS) to Remote Code Execution (RCE).

Technical Summary

Express JS allows developers to use a variety of template rendering engines. These engines substitute things inside the template by inspecting an object that the application has supplied. For example, the following snippet renders a template named “index” and passes an object with two elements, a title, and a message.

```
app.get('/', function (req, res) {
 res.render('index', { title: 'Hey', message: 'Hello there!' })
})
```

Template engines often need a way to set their configuration parameters, such as the path to the template directory, the name of the template, and other engine-specific parameters. To accomplish this many template engines have opted to receive their configuration options directly through the Express render API.

Passing template engine configuration parameters through the Express render API can lead to vulnerabilities if the object is user controlled. Downstream applications often opt to pass their template data in directly through the remote user-controlled `req.query` object. This results in a scenario where a remote attacker may be able to subvert the vulnerable application through malicious template engine configuration options.

The security impact is specific to the engine used by the application but ranges from XSS to RCE.

IMPORTANT: this is a library/engine level API misuse resulting in a **potential** vulnerability in downstream application code. Express did **not** intend for render engines to mix template data with configuration options in the same object. We have confirmed this in discussion with the ExpressJS team.

Real world downstream vulnerabilities manifest when applications pass a user controlled object (e.g. req.query) directly into a render engine that accepts config options through the Express render interface.

Our research has shown that this vulnerability pattern occurs in the wild and that many template engines are following this unintended Express render API pattern of use, resulting in an unknown number of affected downstream applications.

By reporting this API misuse at the engine level, we hope to capture this issue more broadly than trying to pursue every single affected application as well as prevent future API misuse.

Product

express-hbs

Tested Version

2.1.2

Details

Issue: template engine configuration options are passed through Express render API

Express-hbs mixes pure template data with engine configuration options through the Express render API. More specifically, the `layout` parameter may trigger file disclosure vulnerabilities in downstream applications.

This potential vulnerability is somewhat restricted in that only files with existing extentions (i.e. `file.extension`) can be included, files that lack an extension will have `.hbs` appended to them.

Example vulnerable application code:

```
const express = require('express')
const hbs = require('express-hbs')
const app = express()
const port = 3000

app.use(express.urlencoded({ extended: false }));
app.engine('hbs', hbs.express4({
   partialsDir: __dirname
}));

app.set('view engine', 'hbs');
app.set('views', __dirname);
app.get('/', (req, res) => {
   res.render('index', req.query)
})

app.listen(port, () => {
   console.log(`Example app listening at http://localhost:${port}`)
})

module.exports = app;
```

The following POC would retrieve the contents of the `/tmp/test.file` from a vulnerable application:

```
curl "http://localhost:3000?layout=/tmp/test.file"
```

Impact

File disclosure.

Resources

- https://expressjs.com/en/api.html#res.render
- http://expressjs.com/en/guide/using-template-engines.html
- http://expressjs.com/en/advanced/developing-template-engines.html

CVE

- CVE-2021-32817

Resources

- https://github.com/TryGhost/express-hbs#layouts

Credit

This issue was discovered and reported by GHSL team member @agustingianni (Agustin Gianni).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2021-019` in any communication regarding this issue.