

Prototype Pollution

Low dylans published GHSA-3hw5-q855-g6cw on Mar 10, 2020

Package

 **dojox** (npm)

Affected 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

Patched versions

1.16.2, 1.15.3, 1.14.6, 1.13.7, 1.12.8, 1.11.10

Description

The Dojo jQuery wrapper `jqMix` mixin method is vulnerable to Prototype Pollution.

Affected Area:

```
//https://github.com/dojo/dojox/blob/master/jq.js#L442
var tobj = {};
for(var x in props){
  // the "tobj" condition avoid copying properties in "props"
  // inherited from Object.prototype. For example, if obj has a custom
  // toString() method, don't overwrite it with the toString() method
  // that props inherited from Object.prototype
  if((tobj[x] === undefined || tobj[x] != props[x]) && props[x] !== undefined && obj != props[x]){
    if(dojo.isObject(obj[x]) && dojo.isObject(props[x])){
      if(dojo.isArray(props[x])){
        obj[x] = props[x];
      }else{
        obj[x] = jqMix(obj[x], props[x]);
      }
    }else{
      obj[x] = props[x];
    }
  }
}
```

Severity

Low

CVE ID

CVE-2020-5259

Weaknesses

No CWEs