ShwethaKalyanaraman/atom:script/vsts/package.json

Snapshot taken 18 hours ago.

Retest now

Vulnerabilities	1 via 1 paths
Dependencies	198
Source	GitHub
Taken by	Recurring
Tested with	package-lock.json,package.json
Repository	atom
Branch	master
Manifest	script/vsts/package.json

LOW SEVERITY

Prototype Pollution

Vulnerable module: extend

Introduced through: request@2.87.0

Detailed paths and remediation

Introduced through: atom-release-scripts@* › request@2.87.0 › extend@3.0.1

Remediation: Your dependencies are out of date, otherwise you would be using a newer extend than extend@3.0.1. Try reinstalling your dependencies. If the problem persists, one of your dependencies may be bundling outdated modules.

Overview

extend is a port of the classic extend() method from jQuery.

Affected versions of this package are vulnerable to Prototype Pollution. Utilities function can be tricked into modifying the prototype of "Object" when the attacker control part of the structure passed to these function. This can let an attacker add or modify existing property that will exist on all object.

API Status Vulnerability DB Blog Documentation