



# ShwethaKalyanaraman/vscode:extensions/npm/package.json

Snapshot taken [17 hours ago](#).

Retest now

Vulnerabilities	3 via 3 paths
Dependencies	14
Source	GitHub
Taken by	Recurring
Tested with	yarn.lock,package.json
Repository	vscode
Branch	master
Manifest	<a href="#">extensions/npm/package.json</a>

MEDIUM SEVERITY

Access Restriction Bypass

Vulnerable module: [npm](#)

Introduced through: [npm@1.0.1](#)

Detailed paths and remediation

Introduced through: [npm@1.0.1](#)

Remediation: No remediation path available.

Overview

[npm](#) is a JavaScript package manager.

Affected versions of this package are vulnerable to Access Restriction Bypass. It might allow local users to bypass intended filesystem access restrictions due to ownerships of `/etc` and `/usr` directories are being changed unexpectedly, related to a "correctMkdir" issue.

MEDIUM SEVERITY

Symlink attack due to predictable tmp folder names

Vulnerable module: [npm](#)

Introduced through: [npm@1.0.1](#)

Detailed paths and remediation

Introduced through: [npm@1.0.1](#)

Remediation: No remediation path available.

Overview

[npm](#) is a package manager for JavaScript. Affected versions of the package are vulnerable to Symlink attack due to predictable tmp folder names, which were named `/tmp/npm-$PID`. An attacker waiting for a process named `npm` to load could then go to the folder and arbitrarily change the files in the tmp folder.

MEDIUM SEVERITY

npm Taken Lock

## npm token leak

Vulnerable module: [npm](#)

Introduced through: [npm@1.0.1](#)

### Detailed paths and remediation

---

**Introduced through:** npm@1.0.1

**Remediation:** No remediation path available.

### Overview

---

This vulnerability could cause the unintentional leakage of bearer tokens. A design flaw in npm's registry allows an attacker to set up an HTTP server that could collect authentication information, and then use this authentication information to impersonate the users whose tokens they collected. The attacker could do anything the compromised users could do, including publishing new versions of packages.

