snyk Vulnerability DB

Search by package n

Denial of Service (DoS)

Affecting libxmljs package, versions <0.19.8

7.5
HIGH

INTRODUCED: 20 JAN 2022   CVE-2022-21144 ❓

CWE-400 ❓   FIRST ADDED BY SNYK

Share ⌄

Snyk CVSS

Exploit Maturity	**Proof of concept** ❓
Attack Complexity	**Low** ❓
Availability	HIGH ❓

See more

> NVD   7.5 HIGH

How to fix?

Upgrade `libxmljs` to version 0.19.8 or higher.

Overview

libxmljs is a libxml bindings for v8 javascript engine

Affected versions of this package are vulnerable to Denial of Service (DoS). When invoking the `libxmljs.parseXml` function with a non-buffer argument the V8 code will attempt invoking the `.toString` method of the argument. If the argument's `toString` value is not a Function object V8 will crash.

PoC:

```
let libxmljs = require("libxmljs"); let xml =
{toString: 1 }; libxmljs.parseXml(xml);
```
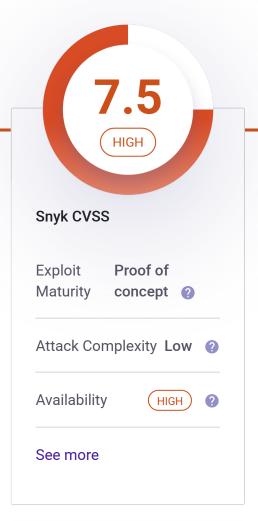
Details

Denial of Service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users.

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.

Unlike other vulnerabilities, DoS attacks usually do not aim at breaching security. Rather, they are focused on making websites and services unavailable to genuine users resulting in downtime.

One popular Denial of Service vulnerability is DDoS (a Distributed Denial of Service), an attack that attempts to clog network pipes to the system by generating a large volume of traffic from many machines.

When it comes to open source libraries, DoS vulnerabilities allow attackers to trigger such a crash or crippling of the service by using a flaw either in the application code or from the use of open source libraries.

Two common types of DoS vulnerabilities:

- High CPU/Memory Consumption- An attacker sending crafted requests that could cause the system to take a disproportionate amount of time to process. For example, commons-fileupload:commons-fileupload.

- Crash - An attacker sending crafted requests that could cause the system to crash. For Example, `npm` `ws` `package`

References

- GitHub Fix Commit
- GitHub PR

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon   Join the >>
             community