

## Arbitrary File Write

Affecting cesanta/mongoose package, versions [7.6)

INTRODUCED: 13 FEB 2022 CVE-2022-25299 ?  
CWE-59 ?

Share ▾

### How to fix?

Upgrade `cesanta/mongoose` to version 7.6 or higher.

### 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

9.8

CRITICAL

### Snyk CVSS

Attack Complexity

Low

?

Confidentiality

HIGH

?

Integrity

HIGH

?

Availability

HIGH

?

[See more](#)

> NVD

7.5 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

- [GitHub Commit](#)

in your application, and 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 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



Join the >>  
community

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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

