



CVE-2022-31022

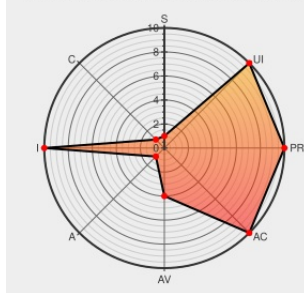
Published on: Not Yet Published

Last Modified on: 06/09/2022 02:13:00 PM UTC

CVE-2022-31022 - advisory for GHSA-9w9f-6mg8-jp7w

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Bleve](#) from [Couchbase](#) contain the following vulnerability:

Bleve is a text indexing library for go. Bleve includes HTTP utilities under bleve/http package, that are used by its sample application. These HTTP methods pave way for exploitation of a node's filesystem where the bleve index resides, if the user has used bleve's own HTTP (bleve/http) handlers for exposing the access to the indexes. For

instance, the CreateIndexHandler (`http/index\_create.go`) and DeleteIndexHandler (`http/index\_delete.go`) enable an attacker to create a bleve index (directory structure) anywhere where the user running the server has the write permissions and to delete recursively any directory owned by the same user account. Users who have used the bleve/http package for exposing access to bleve index without the explicit handling for the Role Based Access Controls(RBAC) of the index assets would be impacted by this issue. There is no patch for this issue because the http package is purely intended to be used for demonstration purposes. Bleve was never designed handle the RBACs, nor it was ever advertised to be used in that way. The collaborators of this project have decided to stay away from adding any authentication or authorization to bleve project at the moment. The bleve/http package is mainly for demonstration purposes and it lacks exhaustive validation of the user inputs as well as any authentication and authorization measures. It is recommended to not use bleve/http in production use cases.

CVE-2022-31022 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **blevesearch** - **bleve** version **>= 0.1.0**

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality	Integrity	Availability

impact

impact

impact

UNCHANGED

NONE

HIGH

NONE

CVSS2 Score:

2.1 - LOW

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Missing Role Based Access Control for the REST handlers in bleve/http package · Advisory · blevesearch/bleve · GitHub

Tags

github.com

text/html

Link

CONFIRM

github.com/blevesearch/bleve/security/advisories/GHSA-9w9f-6mg8-jp7w

Description

Link security advisory to README (#1694) · blevesearch/bleve@1c7509d · GitHub

Tags

github.com

text/html

Link

MISC

github.com/blevesearch/bleve/commit/1c7509d6a17d36f265c90b4e8f4e3a3182fe79ff

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Application

Vendor

Couchbase

Product

Bleve

Version

All

Update

All

Edition

All

Language

All

cpe:2.3:a:couchbase:bleve:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source

@CVEreport

Title

CVE-2022-31022 : Bleve is a text indexing library for go. Bleve includes HTTP utilities under bleve/http package, t... [twitter.com/i/web/status/1...](#)

Posted (UTC)

2022-06-01 19:47:01

Source

@Inceptus3

Title

New Vulnerability: CVE-2022-31022 #InceptusSecure #UnderOurProtection

Posted (UTC)

2022-06-01 22:11:46

Source

@threatmeter

Title

CVE-2022-31022 Bleve is a text indexing library for go. Bleve includes HTTP utilities under bleve/http package, tha... [twitter.com/i/web/status/1...](#)

Posted (UTC)

2022-06-02 07:09:23

Source

/r/netcve

Title

[CVE-2022-31022](#)

Posted (UTC)

2022-06-01 20:38:02

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)