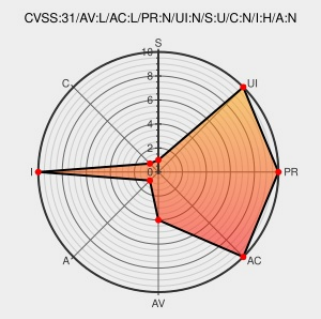
CVE-2022-31022

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



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 Impact**	**Integrity Impact**	**Availability Impact**

Impact	Impact	Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Missing Role Based Access Control for the REST handlers in bleve/http package · Advisory · blevesearch/bleve · GitHub	github.com text/html	CONFIRM github.com/blevesearch/bleve/security/advisories/GHSA-9w9f-6mg8-jp7w
Link security advisory to README (#1694) · blevesearch/bleve@1c7509d · GitHub	github.com text/html	MISC github.com/blevesearch/bleve/commit/1c7509d6a17d36f265c90b4e8f4e3a3182fe79ff

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Couchbase	Bleve	All	All	All	All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	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…	2022-06-01 19:47:01
@Inceptus3	New Vulnerability: CVE-2022-31022 #InceptusSecure #UnderOurProtection	2022-06-01 22:11:46
@threatmeter	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…	2022-06-02 07:09:23
/r/netcve	CVE-2022-31022	2022-06-01 20:38:02

← Previous ID

Next ID→