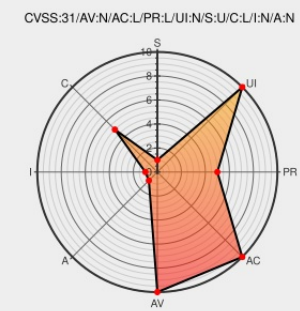
CVE-2022-32169

Published on: Not Yet Published

Last Modified on: 10/03/2022 06:41:00 PM UTC

CVE-2022-32169 - advisory for https://www.mend.io/vulnerability-database/

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bytebase from Bytebase contain the following vulnerability:

The “Bytebase” application does not restrict low privilege user to access “admin issues“ for which an unauthorized user can view the “OPEN” and “CLOSED” issues by “Admin” and the affected endpoint is “/issue”.

CVE-2022-32169 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **bytebase** - **bytebase** version **>= 0.1.0**

Affected Vendor/Software: **bytebase** - **bytebase** version **<= 1.0.4**

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVE References

Description	Tags	Link
bytebase/issue.ts at 1.0.4 · bytebase/bytebase · GitHub	Broken Link, github.com, text/html	MISC github.com/bytebase/bytebase/blob/1.0.4/frontend/src/store/modules/issue.ts#L108-#L187
CVE-2022-32169 | Mend Vulnerability Database	www.mend.io, text/html	MISC www.mend.io/vulnerability-database/CVE-2022-32169

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bytebase	Bytebase	All	All	All	All

cpe:2.3:a:bytebase:bytebase:*:*:*:*:*:*:*:*:

Discovery Credit

Mend Vulnerability Research Team (MVR)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32169 : The “Bytebase” application does not restrict low privilege user to access “admin issues“ for which… twitter.com/i/web/status/1…	2022-09-28 09:40:29
/r/netcve	CVE-2022-32169	2022-09-28 10:38:24

← Previous ID

Next ID→