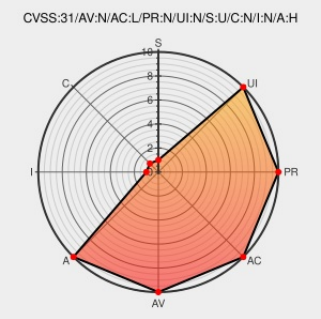
CVE-2022-3212

Published on: Not Yet Published

Last Modified on: 09/16/2022 07:22:00 PM UTC

CVE-2022-3212

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



Certain versions of Axum-core from Axum-core Project contain the following vulnerability:

<bytes::Bytes as axum_core::extract::FromRequest>::from_request would not, by default, set a limit for the size of the request body. That meant if a malicious peer would send a very large (or infinite) body your server might run out of memory and crash. This also applies to these extractors which used Bytes::from_request internally: axum::extract::Form axum::extract::Json String

CVE-2022-3212 has been assigned by security@jfrog.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tokio-rs** - **axum-core** version **< 0.2.8**

Affected Vendor/Software: **tokio-rs** - **axum-core** version **= 0.3.0-rc.1**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
RUSTSEC-2022-0055: axum-core: No default limit put on request bodies › RustSec Advisory Database	rustsec.org text/html	MISC rustsec.org/advisories/RUSTSEC-2022-0055.html
axum-core missing request size limit DoS | - JFrog Security Research	research.jfrog.com text/html	MISC research.jfrog.com/vulnerabilities/axum-core-dos/

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	Vendor	Product	Version	Update	Edition	Language
Application	Axum-core Project	Axum-core	All	All	All	All
Application	Axum-core Project	Axum-core	0.3.0	rc1	All	All

cpe:2.3:a:axum-core_project:axum-core:*:*:*:*:*:rust:*:*:

cpe:2.3:a:axum-core_project:axum-core:0.3.0:rc1:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3212 : <bytes::Bytes as axum_core::extract::FromRequest>::from_request would not, by default, set a limit… twitter.com/i/web/status/1…	2022-09-14 16:08:29
/r/netcve	CVE-2022-3212	2022-09-14 17:38:51

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report