RUSTSEC-2022-0055

History · Edit

No default limit put on request bodies

Reported	August 31, 2022
Issued	September 13, 2022
Package	axum-core (crates.io)
Type	Vulnerability
Categories	denial-of-service
Keywords	#ddos #oom
Details	https://github.com/tokio-rs/axum/pull/1346
Patched	`>=0.2.8, <0.3.0-rc.1` `>=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 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`

The fix is also in `axum-core 0.3.0.rc.2` but `0.3.0.rc.1` *is* vulnerable.

Because `axum` depends on `axum-core` it is vulnerable as well. The vulnerable versions of `axum` are `<= 0.5.15` and `0.6.0.rc.1`. `axum >= 0.5.16` and `>= 0.6.0.rc.2` does have the fix and are not vulnerable.

The patched versions will set a 2 MB limit by default.