Swift-nio-http2 security update: CVE-2023-44487 HTTP/2 DOS

security

lukasa (Cory Benfield) 1 October 10, 2023, 12:12pm

TL;DR: If you run a publicly accessible HTTP/2 server using swift-nio-http2, please update to 1.28.0 *immediately*. If you run any other HTTP/2 server using swift-nio-http2, please update to 1.28.0 as soon as practical.

swift-nio-http2 is vulnerable to a denial-of-service vulnerability in which a malicious client can create and then reset a large number of HTTP/2 streams in a short period of time. This causes swift-nio-http2 to commit to a large amount of expensive work which it then throws away, including creating entirely new s to serve the traffic. This can easily overwhelm an and prevent it from making forward progress.

swift-nio-http2 1.28 contains a remediation for this issue that applies reset counter using a sliding window. This constrains the number of stream resets that may occur in a given window of time. Clients violating this limit will have their connections torn down. This allows clients to continue to cancel streams for legitimate reasons, while constraining malicious actors.

This issue does not particularly affect clients, where the server is limited in its ability to create streams, and is lessened for servers that have loadbalancers or reverse proxies in front of them. In those circumstances, please use this CVE number to find remediations for the relevant software.

The parameters of this sliding window are configurable using APIs introduced in 1.28.0. When the documentation has re-rendered I will update this document with links to the APIs.

9 Likes

How to help fortify swift-nio against DoS?

taylorswift 2 October 10, 2023, 9:03pm

> lukasa:
>
> When the documentation has re-rendered I will update this document with links to the APIs.

for what it's worth, API docs for 1.28.1 are **already available on swiftinit**.

the new APIs can be viewed here:

- `NIOHTTP2Handler.StreamResetFrameRateLimitConfiguration`
- `NIOHTTP2Errors.ExcessiveRSTFrames`

fun fact, swiftinit itself uses swift-nio-http2, **and may have been affected by this as well**.

1 Like