

## CVE ID CPE Description

---

CVE-2021-31618 cpe:2.3:a:apache:http\_server:2.4.47:\*:\*:\*:\*:\* Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server. This issue affected mod\_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released.