Message-ID: <51049a59-5e4b-4def-895f-97b9c2b92b24@oracle.com>
Date: Tue, 10 Oct 2023 11:40:06 -0700
From: Alan Coopersmith <alan.coopersmith@...cle.com>
To: oss-security@...ts.openwall.com
Subject: CVE-2023-44487: HTTP/2 Rapid Reset attack against many
 implementations

[I've seen multiple news articles & blogs in the wake of the coordinated
  disclosure today, but no postings here yet, so lets start fixing that.]

Google, Cloudflare, AWS, and others released details today of a protocol-level
issue in HTTP/2 being exploited in recent months for denial-of-service attacks:

https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
https://aws.amazon.com/blogs/security/how-aws-protects-customers-from-ddos-events/

This attack works via the multiplexed streams feature of HTTP/2, in which the
client repeatedly makes a request for a new stream, and then immediately sends
a RST_STREAM frame to cancel them, resulting in the server doing lots of extra
work to set up and tear down the streams, while not hitting any server-side
limit on a maximum number of active streams per connection.

CVE-2023-44487 was issued to track this issue across implementations:
https://www.cve.org/CVERecord?id=CVE-2023-44487

A script to check for affected implemenations has been posted at:
https://github.com/bcdannyboy/CVE-2023-44487

Information I've found so far on open source implementations (most via the
current listings in the CVE) include:

- Apache httpd:
   https://chaos.social/@icing/111210915918780532

- caddy:
   https://github.com/caddyserver/caddy/issues/5877

- envoy:
   https://github.com/envoyproxy/envoy/pull/30055

- golang:
   https://github.com/golang/go/issues/63417
   https://groups.google.com/g/golang-announce/c/iNNxDTCjZvo

- h2o:
   https://github.com/h2o/h2o/security/advisories/GHSA-2m7v-gc89-fjqf
   https://github.com/h2o/h2o/pull/3291

- haproxy:
   https://github.com/haproxy/haproxy/issues/2312

- hyper:
   https://seanmonstar.com/post/730794151136935936/hyper-http2-rapid-reset-unaffected

- jetty:
   https://github.com/eclipse/jetty.project/issues/10679
   https://github.com/eclipse/jetty.project/releases/tag/jetty-12.0.2
   https://github.com/eclipse/jetty.project/releases/tag/jetty-11.0.17
   https://github.com/eclipse/jetty.project/releases/tag/jetty-10.0.17
   https://github.com/eclipse/jetty.project/releases/tag/jetty-9.4.53.v20231009

- netty:

https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820042a285c5e61

- nghttp2:
  https://github.com/nghttp2/nghttp2/pull/1961
  https://github.com/nghttp2/nghttp2/releases/tag/v1.57.0

- nginx:
  https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/
  https://mailman.nginx.org/pipermail/nginx-devel/2023-October/S36Q5HBXR7CAIMPLLPRSSSYR4PCMWILK.html

- nodejs:
  https://github.com/nodejs/node/pull/50121

- proxygen:
  https://github.com/facebook/proxygen/pull/466

- swift-nio-http2:
  https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764

- tomcat:
  https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M12
  https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14
  https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.81
  https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.94

--
        -Alan Coopersmith-   alan.coopersmith@...cle.com
         Oracle Solaris Engineering - https://blogs.oracle.com/solaris