Security Advisory 2023-074

HTTP/2 Rapid Reset DDoS Vulnerability

October 10, 2023 — v1.3

TLP:CLEAR

History:

- *10/10/2023 — v1.0 – Initial publication*
- *11/10/2023 — v1.1 – Information update based on vendor's advisories*
- *12/10/2023 — v1.2 – Information update based on vendor's advisories*
- *17/10/2023 — v1.3 – Information update based on vendor's advisories*

Summary

On October 10, 2023, Cloudflare, Google and Amazon AWS, jointly disclosed a vulnerability affecting the HTTP/2 protocol [1,2]. Named as `CVE-2023-44487`, this vulnerability impacts various web services and cloud customers. This vulnerability is being actively exploited and has led to Distributed Denial of Service (DDoS) attacks that are significantly larger than previous Layer 7 attacks.

CERT-EU recommends identifying all services using HTTP/2 that are exposed to the Internet, and apply patches or mitigations.

Technical Details

The vulnerability exploits a weakness in the HTTP/2 protocol, allowing attackers to generate hyper-volumetric DDoS attacks. The attack involves sending a large number of HTTP/2 streams and immediately cancelling them, creating a cost asymmetry between the client and server. The attacker exploits the `RST_STREAM` and `GOAWAY` frames of the HTTP/2 protocol to manipulate the connection. This leaves the server doing significant work for cancelled requests while the client pays almost no costs.

Affected Products

All web services and products that use HTTP/2 protocol (nginx, apache, IIS, etc.).

Apache Tomcat

- From version 8.5.0 to version 8.5.93 [3]

Kong

[UPDATE] All supported versions of Kong Gateway, Kong Mesh, and Kuma have been patched [13]. The following versions contain a fix for the HTTP/2 rapid reset attack:

- Kong Gateway Enterprise: 2.8.4.4, 3.1.1.6, 3.2.2.5, 3.3.1.1, 3.4.1.1
- Kong Gateway OSS: 3.4.2
- Kong Mesh: 2.0.8, 2.1.7, 2.2.5, 2.3.3, 2.4.3
- Kuma: 2.0.8, 2.1.7, 2.2.5, 2.3.3, 2.4.3

Unaffected Products

Web applications protected by the following DDoS protection providers or Content Delivery Networks (CDNs) should not be impacted:

- AWS [9]
- Cloudflare [2]
- Google Cloud [1]
- Microsoft Azure [8]
- HAProxy [10]

Detections

Testing if HTTP/2 is enabled

Openssl

```
echo 1 | openssl s_client -alpn h2 -connect google.com:443 -status 2>&1  | grep "ALPN"
```

Nmap

```
nmap -p 443 --script=tls-nextprotoneg <www.google.com>
```

Recommendations

[UPDATE] Apache, Microsoft (IIS and MsQuic), and Kong have issued patches for this vulnerability. It is strongly recommended applying it as soon as possible.

If you are affected, it's recommended to:

- Track connection statistics and identify abusive connections.
- Close connections that exceed the concurrent stream limit, either immediately or after a small number of repeat offenses.
- Implement forceful `GOAWAY` frames to limit stream creation immediately.
- As a last resort, consider disabling HTTP/2 and HTTP/3 to mitigate the threat, although this may result in performance issues.

On the longer terms, it is recommended to use DDoS protection mechanisms.

Mitigations

Since the vulnerability has been recently discovered, all vendors didn't provide advisories yet. This paper will be updated in the next days.

Nginx

Disabling HTTP/2 in NGINX is not necessary. Simply ensure you have configured the following elements :

- `keepalive_requests` should be kept at the default setting of 1000 requests
- `http2_max_concurrent_streams` should be kept at the default setting of 128 streams
- `limit_conn` enforces a limit on the number of connections allowed from a single client. This directive should be added with a reasonable setting balancing application performance and security.
- `limit_req` enforces a limit on the number of requests that will be processed within a given amount of time from a single client. This directive should be added with a reasonable setting balancing application performance and security. [4]

Nginx plans to issue a patch that increases stability under these conditions.

Microsoft IIS and MsQuic

Microsoft published a security update as well as a workaround [7]. CERT-EU recommends using the workaround **only** if you're not able to install the latest updates.

Furthermore, a patch for MsQuic product has been released. CERT-EU recommends updating the MsQuic servers as soon as possible. [12]

Netscaler

Netscaler published recommendations to help reduce the load on backend servers behind Netscaler load balancing and content switching products. CERT-EU recommends carefully considering the impacts of the proposed workarounds before applying them.[11]

General remediations

Remove reference to `http2` in the listening part of the web server configuration file.

References

[1] https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack?hl=en

[2] https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/

[3] https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.94

[4] https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/

[5] https://www.f5.com/company/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products

[6] https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131c66a0c088

[7] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487

[8] https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/

[9] https://aws.amazon.com/blogs/security/how-aws-protects-customers-from-ddos-events/

[10] https://www.haproxy.com/blog/haproxy-is-not-affected-by-the-http-2-rapid-reset-attack-cve-2023-44487

[11] https://www.netscaler.com/blog/news/how-to-mitigate-the-http-2-rapid-reset-vulnerability-on-netscaler/

[12] https://github.com/microsoft/msquic/releases/tag/v2.2.3

[13] https://konghq.com/blog/product-releases/novel-http2-rapid-reset-ddos-vulnerability-update