Health-ISAC™
Collaborating for Resilience in Healthcare
SHARING SINCE 2010

Decoding HTTP/2 Rapid Reset Zero-Day (CVE-2023-44487) Exploited

Threat Bulletins ○ TLP:WHITE Alert ID : c0fe0cdd Oct 10, 2023, 12:16 PM

On October 10, 2023, DDoS Protection firm CloudFlare, in conjunction with Google and Amazon AWS released a statement regarding the discovery of a zero-day vulnerability which could generate massive hyper-volumetric Distributed Denial of Service (DDoS) attacks. The largest attack ever recorded at CloudFlare before the exploit of HTTP/2 Rapid Reset Zero-Day was 71 million requests per second (rps). The attack using the CVE-2023-44487 resulted in an attack which peaked at over 201 million rps.

This zero-day was brought to the attention of Cloudflare in late August 2023 when it was being developed by an unknown threat actor. Later, Cloudflare observed this zero-day exploit being used in conjunction with DDoS botnets to create DDoS attacks with unprecedented volumes.

Health-ISAC is distributing this bulletin for your situational awareness.

Additional Information

Analysis:

The HTTP/2 protocol allows clients to indicate to the server that a previous stream should be canceled by sending an RST_STREAM frame. The protocol does not require the client and server to coordinate the cancellation. The client may also assume that the cancellation will take effect immediately when the server receives the RST_STREAM frame, before any other data from that TCP connection is processed. The HTTP/2 Rapid Reset attack built on this capability is simple: The client opens a large number of streams at once as in the standard HTTP/2 attack, but rather than waiting for a response to each request stream from the server or proxy, the client cancels each request immediately.

The HTTP/2 Rapid Reset attack is named because of its reliance on the ability to send an RST_STREAM frame immediately after sending a request frame. This causes the other endpoint to start working on the request, only to have it rapidly reset. The request is canceled, but the HTTP/2 connection remains open.

Based on a retrospective case study of the incident, Cloudflare was able to extrapolate some insights for cybersecurity leaders moving forward. Some of the most significant knowledge gained from the incident was the illumination of unprecedented potential via use of the Decoding HTTP/2 Rapid Reset Zero-Day vulnerability. It was determined that the record-breaking attack originated from a relatively small botnet made up of approximately 20,000 machines. Cloudflare regularly observes activity stemming from much larger botnets which leads analysts to believe that a large-scale exploit of this zero-day by a large botnet could lead to hyper-volumetric attacks the likes of which have never been observed by Cloudflare.

To read the technical breakdown of the vulnerability in its entirety, please reference the blog post from Cloudflare here.

Mitigation Strategies:

It is recommended that users gain clear visibility into their internet facing applications and those of partner organizations to understand which systems are internet-facing to clearly define their attack surface.

Additionally, members are recommended to employ DDoS protection for layer 7 applications and layer 3 network traffic entities. Firewalls for web apps and API connections are also strongly recommended.

All automation functions should be upgraded to their latest version to minimize the potential for exploitation.

It may be worth investing in a redundant cloud-based DDoS solutions to offer surge protection to internet-facing perimeter applications.

Reference | References

Help Net Security
Google Threat Horizons Report
Business Wire
Security Boulevard
cloudflare

Tags

Exploited, CVE-2023-44487

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base:

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.