HTTP/2 RAPID RESET- CVE-2023-44487

PUBLISHED: OCTOBER 18, 2023 | LAST UPDATE: OCTOBER 18, 2023

Summary

On October 10, 2023, the HTTP/2 Rapid Reset Vulnerability CVE-2023-44487 was published. The HTTP/2 Rapid Reset Vulnerability leverages the characteristics of the HTTP/2 protocol. This vulnerability allows attackers to exploit the HTTP/2 protocol's design, leading to a DDoS attack vector. Unlike HTTP/1.1, HTTP/2 permits multiplexing, where multiple data streams can be established within a single TCP connection. The vulnerability can allow malicious actors to bypass server limits on data streams by issuing reset stream packets immediately after requesting a new stream. The servers may fail to clean up closed streams promptly, placing stress on the servers. Some bot exploits are known to request a large number of streams within a single TCP connection.

This issue only affects HTTP/2 server systems and does not affect HTTP/1.1 or 1.0 server systems. The A10 Networks ACOS Management Web User Interface uses HTTP/1.1 and does not use HTTP/2. The ACOS TPS systems inspect HTTP/2 traffic but do not process HTTP/2 connection, reset, or any control frames. Accordingly, these systems are not exposed to this vulnerability.

A10 Networks ACOS ADC Data Plane can process HTTP/2 control frames and is protected by configurable control frame limits built into the HTTP2 processing. This protection will close connections that exceed the configured limits.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2023-44487	CVSSv3	7.5 High	HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack) [1]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated recommended resolved release or a newer release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected	Releases Recommended, Resolved or Unaffected
4.1.4 - 4.1.4-GR1-P2	4.1.4-GR1-P10 5.2.1-P6 6.0.1, 6.0.2

Workarounds and Mitigations

A10 Networks ACOS ADC Configuration

A10 Networks ADC have built in control frame limits and will close connections that exceed these limits. The default control frame limit is 10,000. This can be configured to a lower number. The limit to use will depend on the system configuration and traffic presented. Considering the current Rapid Reset attack, a low limit of 500, 100, 50 or 10 can be used for greater protection.

©2023 A10 Networks, Inc. All rights reserved.

To configure the frame limit for a slb server, use the following frame-limit command for its slb template.

```
frame-limit: Limit the number of CONTINUATION, PING, PRIORITY, RESET, SETTINGS and empty frames in one
HTTP2 connection, default 10000

      slb template http <NAME>
        frame-limit 50
```

The show `slb http2 detail` command can be used to view http2 detailed counters including `RST_STREAM Frame Rcvd` and `Frame Flood Detected`. Monitoring these counters can assist in determining if an attack has occurred or is occurring.

To evaluate an optimized setting for a specific environment, review the ratio of Transactions per Second (tps) over Connections per Second (cps) or tps/cps. This can be derived from the counters shown by the `slb http2 detail` command by adding the totals of `PRIORITY Frame Rcvd` + `PING Frame Rcvd` + `CONTINUATION Frame Rcvd` / `Total HTTP2 Session`. A typical environment may have a ratio of between 1.5 to 2. Setting the frame-limit to 100 for these cases provides good protection and should not interfere with typical traffic patterns. A lower setting of 50 or 10 should also not interfere with the typical traffic for these cases.

Additional Mitigation for HTTP servers

IP Blocklists

Regularly updating and maintaining IP blocklists to block traffic from known botnets is a fundamental security practice. Blocking traffic from participating botnets during an attack can substantially mitigate the threat.

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

©2023 A10 Networks, Inc. All rights reserved.

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2022-44487	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Related Links

Ref #	General Link
[1]	http://nvd.nist.gov/vuln/detail/CVE-2023-44487

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2023-10-18	Initial Publication

© Copyright 2023 A10 Networks, Inc. All Rights Reserved.

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.