Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

HTTP/2 Zero-Day Exploited for the Most Explosive DDoS Attacks

Date of Publication	Admiralty Code	TA Number
October 11, 2023	A1	TA2023409

Summary

First Seen: August 2023
Affected Products: HTTP/2 servers
Impact: A zero-day vulnerability in HTTP/2 has been actively exploited in August, introducing a novel DDoS technique referred as "Rapid Reset". The attack, utilizing CVE-2023-44487, exploits a vulnerability within the HTTP/2 protocol and enables remote attackers to carry out a denial of service (DoS) attack.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability	HTTP/2 Servers	✓	✓	✓

Vulnerability Details

#1 A new DDoS (distributed denial of service) technique, known as 'HTTP/2 Rapid Reset,' has been actively exploited as a zero-day vulnerability (CVE-2023-44487) since August. This attack method has surpassed previous records in terms of its scale and impact. 'HTTP/2 Rapid Reset' exploits a zero-day flaw in the HTTP/2 protocol, allowing attackers to conduct DDoS attacks.

#2 CVE-2023-44487 is a vulnerability that is believed to impact every web server implementing HTTP/2. HTTP/2 is known for its capability to multiplex requests over a single TCP connection, allowing concurrent streams. This vulnerability is connected to the exploitation of this multiplexing feature for Distributed Denial of Service (DDoS) attacks.

#3

The vulnerability, CVE-2023-44487, arises from improper control of resource consumption when processing HTTP/2 requests that include compressed HEADERS frames. Exploiting this vulnerability involves sending compressed HEADERS frames followed by rapid cancellation with RST_STREAM frames, leading to server resource exhaustion and service disruption.

#4

In recent incidents, notable organizations have experienced massive DDoS attacks that exploited the HTTP/2 Rapid Reset vulnerability. Google reported a peak attack rate of 398 million requests per second (RPS), which is over seven times larger than any previous attack they had encountered. Cloudflare observed an attack three times larger than their previous record of 71 million RPS. Amazon, too, faced numerous HTTP/2 Rapid Reset attacks, with the largest one peaking at 155 million RPS over a two-day period in late August. These attacks highlight the magnitude and severity of the exploitation of the CVE-2023-44487 vulnerability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-44487	Microsoft IIS: 10.0, Apache Tomcat: 8.5.0 - 11.0.0-M11, Netty: 4.0.0 - 4.1.99, Jetty: 9.0.0.v20130308 - 12.0.1	cpe:2.3:o:microsoft:IIS:10.0:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_tomcat:11.0.0-M11:*:*:*:*:*:*:* cpe:2.3:a:netty:netty:4.1.99:*:*:*:*:*:*:* cpe:2.3:a:eclipse:jetty:9.4.53.v20230927:*:*:*:*:*:*:*	CWE-400

Recommendations

Update Server: Ensure that any servers you operate, which support HTTP/2, are not vulnerable to the CVE-2023-44487 attack. Apply vendor-supplied patches which will mitigate the risks associated with this attack vector.

DDoS Mitigation Services: Consider using DDoS mitigation services or appliances to help absorb and filter out malicious traffic during large-scale DDoS attacks.

Traffic Monitoring and Anomaly Detection: Continuously monitor network and server traffic for unusual patterns or sudden spikes in traffic. Anomaly detection can help you identify potential attacks in real-time.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0040** Impact	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1498 Network Denial of Service	**T1584** Compromise Infrastructure	**T1584.005** Botnet	

Patch Details

It is recommended that any servers which the organization runs that support HTTP/2 are updated with the vendor patches for addressing the CVE-2023-44487.

Update the Microsoft provided workarounds and patches to mitigate the flaw
Link:
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-44487

Updates by netty for the fixed version 4.1.100 addressing the flaw.
Link:
https://netty.io/downloads.html

Update your jetty servers to- version 1.28.0
Link:
https://mvnrepository.com/artifact/org.eclipse.jetty/jetty-servlets/9.4.53.v20231009

References

https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

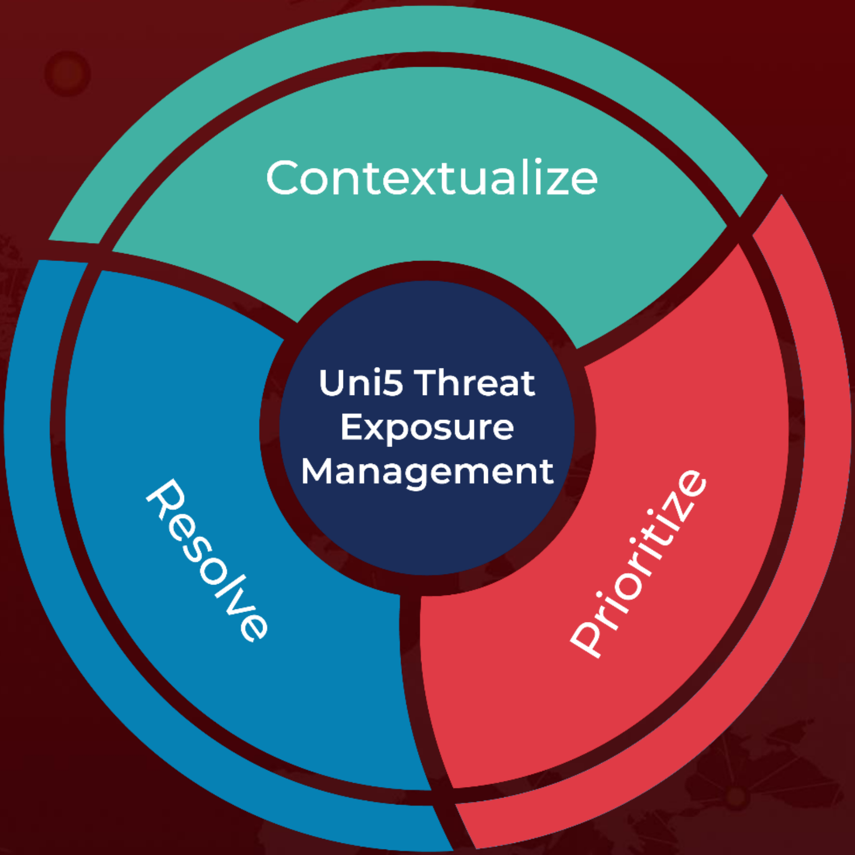
https://aws.amazon.com/blogs/security/how-aws-protects-customers-from-ddos-events/

https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 11, 2023 • 5:20 AM

More at www.hivepro.com