FORTINET

OUTBREAK ALERTS

HTTP/2 Rapid Reset Attack

Zero-Day DDoS vulnerability exploited in the wild

https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
CVEs: CVE-2023-44487

A newly identified Distributed Denial-of-Service (DDoS) attack technique is used in the wild. This DDoS attack, known as 'HTTP/2 Rapid Reset', leverages a flaw in the implementation of protocol HTTP/2.

Background

HTTP/2 is a connection-oriented application-layer protocol that runs over a TCP connection ([TCP]). HTTP/2 enables a more efficient use of network resources and a reduced latency by introducing field compression and allowing multiple concurrent exchanges on the same connection.

The attack sends a set number of HTTP requests, to generate a high volume of traffic on the targeted HTTP/2 servers. Attackers can cause a significant increase in the request per second and high CPU utilization on the servers that eventually can cause resource exhaustion causing denial of service.

Announced

Oct 10, 2023: According to a Google blog post the largest attack reached up to 398 million requests per second.
https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

Oct 10, 2023: CISA released an advisory for this DDoS attack.
https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487

Oct 11, 2023: FortiGuard released a Threat Signal on the vulnerability (CVE-2023-44487)
https://www.fortiguard.com/threat-signal-report/5286/http-2-rapid-reset-attack

Latest Developments

Oct 12, 2023: FortiGuard has released an IPS signature to detect and block attacks targeting the denial of service vulnerability on HTTP/2 protocol (CVE-2023-44487)

FortiGuard recommends using application layer protection service such as Web Application Firewall (WAF) to protect web applications against network attacks. Also, recommends using Application Delivery service for load balancing and generally improving security posture.
https://www.fortinet.com/products/web-application-firewall/fortiweb
https://www.fortinet.com/products/application-delivery-controller/fortiadc

Additionally FortiWeb customers should use HTTP Protocol Constraints to define/reduce the max number of requests per client. See the instruction listed on this article:
https://community.fortinet.com/t5/FortiWeb/Technical-Tip-How-to-Enable-HTTP-2-Max-Requests-in-HTTP-Protocol/ta-p/278958

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

Vulnerability

Detects vulnerable application related to CVE-2023-44487 Denial of Service Vulnerability

FortiClient
DB 1.552

- **Exploitation**

IPS

Detects and block attacks targeting the denial of service vulnerability on HTTP/2 protocol (CVE-2023-44487)

FortiGate *DB 25.655* | FortiSASE *DB 25.655* | FortiNDR *DB 25.655* | FortiADC *DB 25.655* | FortiProxy *DB 25.655*

Web App Security

Use HTTP Protocol Constraints to define/reduce the max number of requests per client.

FortiWeb
v7.4.0

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient *DB 1.00015* | FortiAnalyzer *DB 2.00022* | FortiSIEM *v6.6+*

Threat Hunting

FortiAnalyzer
v6.4

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiEDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response | FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training | Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

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

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

Security Week https://www.securityweek.com/rapid-reset-zero-day-exploited-to-launch-largest-ddos-attacks-in-history/

The Stack https://www.thestack.technology/http2-rapid-reset-record-ddos/

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/

Learn more about FortiGuard Outbreak Alerts