Search blog

Blog Home

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

Allow all

Customize

Reject all

reveal their experiences mitigating powerful HTTP/2-based DDoS attacks utilizing a zero-day technique referred to as 'Rapid Reset', documented under the vulnerability identifier CVE-2023-44487. The attack magnitudes reported are astonishing: Amazon mitigated attacks at a rate of 155 million requests per second, Cloudflare at 201 million rps, and Google endured a record-breaking 398 million rps. This vulnerability was under active attack in August.

What is CVE-2023-44487 HTTP/2 Rapid Reset Attack?

The 'Rapid Reset' technique leverages the 'stream multiplexing' feature of HTTP/2, wherein numerous requests and subsequent immediate cancellations cause substantial server-side workload with minimal client-side attacker cost. The attack takes advantage of a feature in HTTP/2 by repeatedly sending and canceling requests, which overwhelms the target website or application, causing it to stop working correctly. HTTP/2 has a

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

various mitigative strategies. Implementing rate controls is pivotal in managing the effects of the attacks since they exploit the protocol directly and lack a one-size-fits-all solution. Critically, the underpinning preventive measure across all defenses is the vital and timely updating and patching of systems. Customers should update their systems with available patches to strengthen against this vulnerability, ensuring a robust barrier against exploitative attacks.

How can Qualys Help?

Addressing the risks of CVE-2023-44487, or the HTTP/2 Rapid Reset Attack, starts with identifying vulnerable assets. Utilize the following QIDs to aid this matter.

QID	Title	VulnSigs Version
45475	Apache http2 module Detected	VULNSIGS-2.5.87.2-1
45266	Web Server HTTP Protocol Versions	VULNSIGS-2.4.25-2

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›

Mitigation refers to a setting, common configuration, or general best practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability.

A **workaround** is a method, sometimes used temporarily, for achieving a task or goal when the usual or planned method isn't working. Information technology often uses a workaround to overcome hardware, programming, or communication problems. Once a problem is fixed, a workaround is usually abandoned.

The following Qualys Policy Compliance Control IDs (CIDs), and System Defined Controls (SDC) have been updated to support recommended mitigation(s):

For Windows and IIS technology:

- 17331 Status of the 'HTTP/2' feature on the host (EnableHttp2Cleartext)
- 17330 Status of the 'HTTP/2' feature on the host (EnableHttp2Tls)

For F5 BIG-IP technology:

- 26840 Status of the 'concurrent-streams-per-connection' setting configured for the ltm http2 profile

For Nginx technology:

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

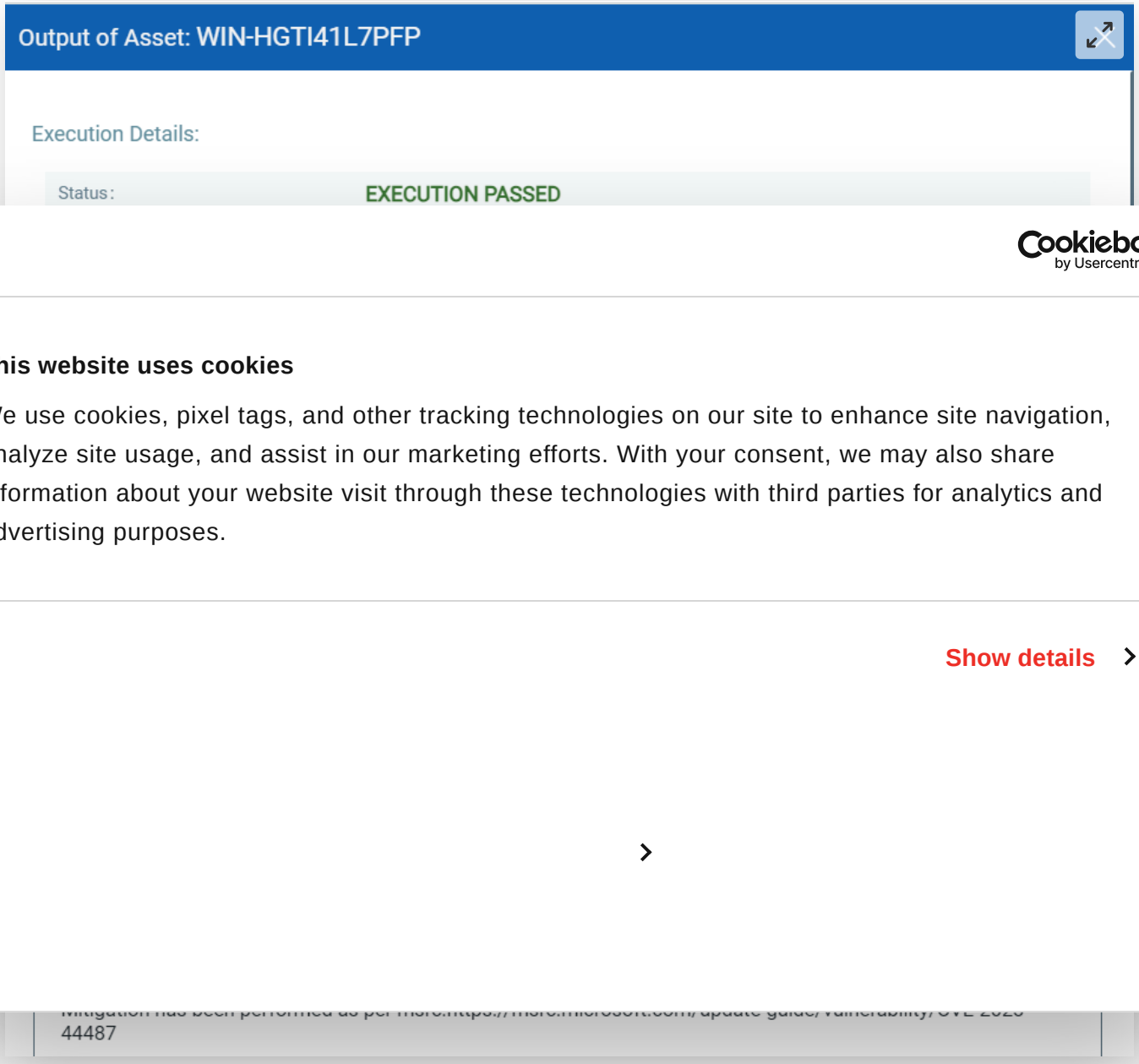
- 26906 Status of HTTP2 on Http profile

Execute Mitigation Using Qualys Custom Assessment and Remediation (CAR)

Qualys Custom Assessment and Remediation (CAR) can be leveraged to execute mitigation.

Try Qualys CAR for free

For Windows and IIS technology



Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

CAR team is addressing the introduced mitigation/workaround from other supported technologies and will provide an update once scripts are added to the library.

Note: Scripts will be available in the CAR script library.

Detecting Vulnerability with Qualys WAS

Customers can launch WAS scan and if their Apache tomcat servers are vulnerable, QID 150732 will be reported. The QID is detected based on installed version.

The information below showcases the HTTP request and response used to identify the above-mentioned vulnerability. This detection was made possible using the Qualys Web Application Scanning (WAS) system, specifically with the QID 150732.

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›



Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

Additional Contributors:

- Xiaoran (Alex) Dong, Manager, Compliance Signature Engineering, Qualys
- Sheela Sarva, Director, Quality Engineering, Web Application Security, Qualys



Written by
Saeed Abbasi, Head of Threat Research Unit (TRU), Director of Product, Qualys
Write to Saeed at sabbasi@qualys.com

Share

Related content
rapid reset attack

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

Start a discussion

Follow us on

Company
About Us
Investor Relations
Partners
Events
Awards
Customers
Careers

Platform
Overview
Use Cases
Segments
Free Trials

Resources
Threat Research Unit
Blog
Resource Library
Sitemap
Support
Community
Release Notes

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›