NST ASSURE
Continuous Threat Exposure Management

SECURITY ADVISORY

HTTP/2 CONTINUATION Flood Vulnerability

DATE: 05 April 2024

Security Advisory: HTTP/2 CONTINUATION Flood Vulnerability

This is a general security advisory on the trending High DoS Vulnerability on HTTP/2

Date: **April 05, 2024**

Vulnerability: **HTTP/2 CONTINUATION Flood Vulnerability**

CVE Identifier: amphp/http **(CVE-2024-2653)**, Apache HTTP Server **(CVE-2024-27316)**, Apache Tomcat **(CVE-2024-24549)**, Apache Traffic Server **(CVE-2024-31309)**, Envoy proxy **(CVE-2024-27919 and CVE-2024-30255)**, Golang **(CVE-2023-45288)**, h2 Rust crate, nghttp2 **(CVE-2024-28182)**, Node.js **(CVE-2024-27983)**, and Tempesta FW **(CVE-2024-2758).**

CVSS Score: **Not yet assigned**

What is it ?

Recently, a vulnerability has been discovered in the HTTP/2 protocol, known as HTTP/2 CONTINUATION Flood. This vulnerability allows attackers to launch Denial-of-Service (DoS) attacks against vulnerable web servers.

An attacker can exploit this vulnerability by sending a malicious stream of CONTINUATION frames within an HTTP/2 request. These frames lack the terminating END_HEADERS flag, causing the server to allocate excessive memory and processing power to parse incomplete headers. This can lead to a DoS attack, rendering the server unavailable to legitimate users.

Affected Systems

Web servers that implement the HTTP/2 protocol are potentially vulnerable, especially if they do not properly handle CONTINUATION frames.

Specific vendor products or versions haven't been definitively identified yet. However, most major web server software is likely at risk until patched.

Impact

A successful HTTP/2 CONTINUATION Flood attack can have a significant impact on enterprise environments, including:

Service Disruption: The attack can render web servers unavailable to legitimate users, causing website outages and potential financial losses.

Performance Degradation: Even if the server doesn't completely crash, the attack can significantly degrade server performance, impacting user experience and potentially affecting other critical applications.

Reputational Damage: Frequent DoS attacks can damage an organization's reputation and erode user trust.

Mitigation

Apply Patches Promptly: Patching your web server software with the latest updates is the most effective mitigation strategy.

Mitigation

Disable HTTP/2 (if acceptable): If your environment can tolerate disabling HTTP/2 temporarily, consider doing so until a permanent patch is available. However, this might have compatibility implications for some applications.

Additional Information

Reference Links:

- https://httpd.apache.org/security/vulnerabilities_24.html
- https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg
- https://github.com/envoyproxy/envoy/security/advisories/GHSA-gghf-vfxp-799r
- https://github.com/amphp/http/security/advisories/GHSA-qjfw-cvjf-f4fm
- https://github.com/nghttp2/nghttp2/security/advisories/GHSA-x6x3-gv8h-m57q
- https://pkg.go.dev/vuln/GO-2024-2687
- https://github.com/tempesta-tech/tempesta/security/advisories/GHSA-3xwj-5ch3-q9p4

NST ASSURE
Continuous Threat Exposure Management

99 S Almaden Blvd, Suite 600,
San Jose CA 95113

info@nstcyber.ai

www.nstcyber.ai

About NST Cyber

NST Cyber is a leading provider of Continuous Threat Exposure Management (CTEM) to Large Enterprises. Utilizing advanced Artificial Intelligence (AI) and Machine Learning (ML), NST Assure CTEM continuously detects exposed assets and vulnerabilities. It prioritizes risk based on potential attack patterns and exploitability, taking proactive measures to mitigate them before they can be exploited by malicious actors.