Advisory: Critical vulnerability in Critical Apache HTTP/2 Flaw

This is an urgent security advisory regarding a critical security vulnerability related to HTTP/2 Flaw. The Apache Software Foundation has patched a high-severity security flaw in the Apache HTTP Server that could allow attackers to execute code remotely. This vulnerability poses a high risk to availability, particularly for government portals, banking and financial services, public-facing APIs, and critical infrastructure systems. Therefore, immediate action is required to ensure the continued security and availability of affected services.

Summary of Critical Vulnerability

- **Vulnerability Name:** Apache HTTP/2 DoS / Protocol Handling Flaw (**CVE-2026-23918**)
- **Severity:** Critical (CVSS ~9.8–10.0, depending on configuration)
- **Type:** Denial of Service (DoS) / Potential Resource Exhaustion
- **Affected Component:** Apache HTTP Server (mod_http2)
- **Root Cause:** Improper handling of HTTP/2 requests leading to excessive resource consumption and connection mismanagement
- **Impact:**
    - Remote attackers can exploit the flaw by sending specially crafted HTTP/2 requests
    - Can cause **service disruption**, **thread exhaustion**, or **server crash**
    - May affect availability of critical web services
- **Attack Vector:** Network (Unauthenticated, remote exploitation possible)
- **Status:** Publicly disclosed; active exploitation risk is high due to ease of triggering
- **Affected Systems**
    - Apache HTTP Server instances with:
        - **HTTP/2 (mod_http2) enabled**
        - Default or misconfigured request handling limits
    - Likely affected versions include:
        - Apache HTTP Server **2.4.x versions prior to patched releases** (exact versions to be confirmed via vendor advisory)

Technical Overview

The vulnerability arises from improper handling of HTTP/2 streams and request frames. Attackers can *Open multiple HTTP/2 streams rapidly*, *Send crafted or incomplete frames*, or *Force the server to allocate excessive resources (memory/threads)*, which could lead to:

- Resource exhaustion
- Connection saturation
- Service degradation or complete denial of service

Recommendations for Urgent Action

All organizations running Apache HTTP Server with HTTP/2 enabled must take **immediate action** as noted below:

1. Apply Security Patches

- Upgrade Apache HTTP Server to the **latest patched version** (as released by Apache Foundation)
- Monitor official Apache advisories for confirmed fixed versions

2. Disable HTTP/2 (Temporary Mitigation)

If patching is not immediately possible, do the following:

- Disable HTTP/2 module (`mod_http2`)
- Revert to HTTP/1.1 until mitigation is applied

3. Harden Server Configuration

- Limit concurrent HTTP/2 streams
- Configure request timeout and connection limits
- Tune `MaxRequestWorkers`, `H2MaxSessionStreams`, and related directives

4. Deploy Network Protections and monitor

- Use Web Application Firewalls (WAF) to detect abnormal HTTP/2 traffic patterns
- Apply rate limiting and anomaly detection
- Monitor logs for:
    - Sudden spikes in HTTP/2 connections
    - High resource utilization
    - Repeated malformed requests
- Enable alerting for abnormal traffic behavior

References

1. https://thehackernews.com/2026/05/critical-apache-http2-flaw-cve-2026.html
2. https://nvd.nist.gov/vuln/detail/CVE-2026-23918
3. https://www.cve.org/CVERecord?id=CVE-2026-23918