ultraviolet

THREAT ADVISORY

Apache HTTPD Vulnerability CVE-2026-23918

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
May 6, 2026
TLP:GREEN

Executive Snapshot

CVE-2026-23918 is a critical double-free vulnerability (CVSS 8.8) in the mod_http2 module of Apache HTTP Server 2.4.66, disclosed on May 5, 2026, and patched in version 2.4.67. The flaw allows an unauthenticated remote attacker to crash a worker process with just two HTTP/2 frames over a single TCP connection, producing a trivially repeatable denial-of-service condition. Under specific but common deployment configurations, particularly Debian-derived systems and the official httpd Docker image, the same flaw can be escalated to full remote code execution by exploiting predictable memory layouts in the Apache Portable Runtime. Because mod_http2 ships enabled by default and the attack requires no credentials, special headers, or targeted URLs, the exposed surface is broad, and the barrier to exploitation is low. Organizations running Apache 2.4.66 with HTTP/2 enabled on any internet-facing or internally accessible endpoint should treat this as an emergency remediation priority.

- **Patch immediately.** Upgrade all Apache HTTP Server instances to version 2.4.67, including containerized deployments built on the official httpd Docker image, and bypass standard change windows where risk tolerance permits.
- **Apply interim mitigations where patching is delayed.** Disable mod_http2 to fall back to HTTP/1.1, or switch from a multi-threaded MPM to MPM prefork, which is not affected by this flaw. Neither workaround is a long-term substitute for the patch.
- **Instrument and monitor.** Deploy network-level detection for anomalous HTTP/2 RST_STREAM patterns and conduct an asset inventory to ensure full coverage of affected versions across the environment, paying particular attention to default configurations that may have gone unaudited.

TIDE Team Analysis

On May 5, 2026, the Apache Software Foundation disclosed CVE-2026-23918, a double-free vulnerability in the mod_http2 module of Apache HTTP Server version 2.4.66. Assigned a CVSS score of 8.8, the flaw can lead to both denial-of-service and remote code execution. The vulnerability has been resolved in version 2.4.67. Given the ubiquity of Apache in enterprise web infrastructure, this vulnerability warrants immediate attention from security leadership.

The root cause lies in the stream cleanup logic within h2_mplx.c. When a client sends an HTTP/2 HEADERS frame immediately followed by a RST_STREAM with a non-zero error code on the same stream, two internal callbacks fire in sequence before the multiplexer has registered the stream. Both callbacks push the same h2_stream pointer onto the cleanup array, and when the purge function later iterates and calls apr_pool_destroy on each entry, the second call operates on already-freed memory. This is a textbook double-free condition (CWE-415) that corrupts heap metadata and opens the door to attacker-controlled behavior.

The denial-of-service path is trivial to exploit. It requires only a single TCP connection, two frames, no authentication, no special headers, and no specific URL. The targeted worker process crashes on every attempt. While Apache respawns the worker, every in-flight request handled by that process is dropped. An attacker can sustain this pattern indefinitely, creating persistent service degradation that is difficult to distinguish from intermittent infrastructure failure without deep packet inspection.

The remote code execution path is more constrained but demonstrably practical. A working proof-of-concept has been validated on x86_64, leveraging mmap allocator reuse in the Apache Portable Runtime (APR), which is the default configuration on Debian-derived systems and the official httpd Docker image. The exploit chain places a fake h2_stream struct at the freed virtual address, redirects the pool cleanup function pointer to system(), and uses Apache's scoreboard memory as a stable container for the payload. Because the scoreboard resides at a fixed address for the lifetime of the server process regardless of ASLR, the technique bypasses standard memory randomization defenses. In lab conditions, execution reportedly lands within minutes.

The organizational impact of this vulnerability is significant. Apache HTTP Server remains one of the most widely deployed web servers globally, and mod_http2 ships in default builds with HTTP/2 commonly enabled in production. Any internet-facing Apache 2.4.66 instance with mod_http2 active and a multi-threaded MPM is exposed. The low complexity of the DoS vector means that even unsophisticated threat actors can weaponize this flaw, while the RCE path raises the stakes for organizations running Debian-based or Docker-based Apache deployments. Exploitation requires no authentication and targets a protocol-level handler, meaning WAF rules and application-layer controls offer limited protection.

There is a narrow mitigation for organizations unable to patch immediately. The MPM prefork model is not affected by this flaw, so switching to prefork could serve as a temporary workaround. However, prefork carries its own performance limitations and is not suitable for high-concurrency environments. Disabling mod_http2 and falling back to HTTP/1.1 would also eliminate the attack surface, though at the cost of protocol efficiency. Neither workaround is a substitute for patching.

Security leadership should prioritize the following actions. First, conduct an immediate asset inventory to identify all Apache HTTP Server 2.4.66 instances across the environment, including containerized deployments using the official

httpd Docker image. Second, escalate patching to version 2.4.67 as an emergency change, bypassing standard release windows where risk tolerance permits. Third, for systems that cannot be patched within 24 to 48 hours, apply the interim mitigations of disabling mod_http2 or switching to MPM prefork. Fourth, monitor network telemetry for anomalous HTTP/2 RST_STREAM patterns that may indicate exploitation attempts.

This vulnerability reinforces the need for continuous visibility into server-side software versions and default module configurations. The combination of unauthenticated network access, trivial DoS, and a viable RCE chain against common deployment defaults makes CVE-2026-23918 one of the more consequential Apache vulnerabilities in recent years. Organizations that delay remediation accept material risk of service disruption and potential compromise of web-tier infrastructure.

Why It Matters

CVE-2026-23918 presents a direct risk to containerized workloads. The official httpd Docker image ships with the APR mmap allocator configuration that enables the RCE exploit path. Organizations that use this image as a base layer in CI/CD pipelines will continue to build and deploy vulnerable containers until the image reference is updated. In Kubernetes and similar orchestration platforms, this means the vulnerability can be present across hundreds of pods simultaneously, and ephemeral container lifecycles often fall outside the scope of traditional host-based vulnerability scanning. If containers run with elevated privileges or share host namespaces, a compromised Apache process provides a viable entry point for lateral movement within the cluster.

Apache HTTP Server has a documented history of critical vulnerabilities that were exploited rapidly after disclosure. CVE-2021-41773 and CVE-2021-42013 were weaponized within days, and the HTTP/2 protocol handler specifically has been a repeated source of flaws, including the 2023 rapid reset attack (CVE-2023-44487). mod_http2 ships enabled in default Apache builds, and HTTP/2 is widely activated in production, which means the default attack surface for CVE-2026-23918 is large without any misconfiguration required on the part of the operator.

Patch management at the WAN-facing perimeter is the primary control for this class of vulnerability. The flaw requires no authentication and is exploitable over the network with minimal complexity, so internet-exposed Apache 2.4.66 instances are at immediate risk from the moment exploit tooling becomes available. Security teams should confirm that perimeter asset inventories account for both traditional deployments and containerized instances, that container base image policies enforce version pinning against patched releases, and that emergency patch SLAs for critical findings are defined and enforceable.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure all Apache2 HTTPD services are not running version 2.4.66, update to 2.4.67 or downgrade to an earlier version.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---