INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 09:04 UTC

Critical Apache HTTP/2 Double-Free Flaw (CVE-2026-23918) Enables DoS and Potential RCE

CVE VULNERABILITY | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0129
Type	CVE Vulnerability
CVE ID	CVE-2026-23918
Severity	CRITICAL
CVSS Base Score	9.1
EPSS Score	0.0006 (19th percentile)
Affected Products	Apache HTTP Server (HTTP/2 module, exact version range unconfirmed from available data; see CVE record at cve.org for authoritative version scope)
Published	19 hours ago
Discovery Source	Serper

Executive Summary

Apache has released a security update addressing CVE-2026-23918, a critical memory management flaw in the HTTP/2 module of Apache HTTP Server. An unauthenticated remote attacker could exploit this flaw to crash affected servers (confirmed DoS). RCE potential has been reported by security researchers and cPanel but is unconfirmed by NIST/NVD technical review. Organizations running Apache HTTP Server with HTTP/2 enabled, including managed hosting environments using cPanel, should treat this as a priority patching event.

Technical Analysis

CVE-2026-23918 is a double-free vulnerability (CWE-415) in Apache HTTP Server's HTTP/2 request handler. A double-free condition occurs when a memory allocation is freed more than once, corrupting the heap and potentially enabling attacker-controlled code execution. Attack vector is network-based, requires no authentication, and no user interaction. Reported CVSS base score: 9.1 (critical). EPSS score: 0.00061 (18.8th percentile), indicating low observed exploitation probability at time of data capture, though EPSS lags real-world exploitation curves for newly disclosed critical CVEs. MITRE technique mapping: T1499 (Endpoint Denial of Service) and T1190 (Exploit Public-Facing Application). RCE potential is assessed low-to-medium confidence pending NVD and Apache Security Advisory confirmation. Affected version range is unconfirmed from available

data, the authoritative version scope must be obtained from the CVE record at cve.org/CVERecord?id=CVE-2026-23918 or the NVD entry at nvd.nist.gov/vuln/detail/CVE-2026-23918. cPanel has published a support advisory confirming downstream impact on managed hosting deployments. No public proof-of-concept or active exploitation confirmed at time of data capture. CISA KEV listing: not present.

Action Checklist

1. Step 1: Containment, Identify all Apache HTTP Server instances in your environment with HTTP/2 enabled (check Apache config for 'Protocols h2' or 'h2c' directives). If patching cannot begin immediately, consider temporarily disabling HTTP/2 on externally facing servers by removing 'h2' from the Protocols directive and restarting Apache. Confirm affected version range from the CVE record at cve.org or the Apache Security Advisory before scoping containment.
2. Step 2: Detection, Query asset inventory and CMDB for Apache HTTP Server deployments. Check web server access and error logs for anomalous HTTP/2 connection patterns, repeated connection resets, or segmentation fault entries in Apache error logs (error.log). Review WAF and IDS/IPS logs for unusual traffic volumes to HTTP/2 endpoints. No confirmed IOC signatures are available at time of data capture.
3. Step 3: Eradication, Apply the Apache Software Foundation's official patch for CVE-2026-23918. Retrieve the authoritative patch from the Apache Security Advisory (httpd.apache.org, verify this URL resolves to the official advisory page before proceeding) or request the CVE record directly from cve.org/CVERecord?id=CVE-2026-23918. For cPanel-managed environments, apply the cPanel security update per the advisory at support.cpanel.net/hc/en-us/articles/40229402602519-Security-CVE-2026-23918.
4. Step 4: Recovery, After patching, confirm the Apache service starts without error and HTTP/2 functionality operates normally. Review error logs for any residual crash indicators. Retest externally facing services with an HTTP/2 client to confirm normal response. If HTTP/2 was temporarily disabled as a containment measure, re-enable only after the patch is applied and verified.
5. Step 5: Post-Incident, Review your patch SLA against the time elapsed between disclosure and remediation for this CVE. Assess whether HTTP/2-enabled Apache instances are included in your external attack surface inventory. Evaluate whether your WAF or IPS has signatures covering malformed HTTP/2 request patterns as a compensating control for future HTTP/2-layer vulnerabilities.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and initiate formal incident declaration if Apache error.log contains segmentation fault entries (indicating active exploitation attempts triggering the CVE-2026-23918 double-free condition), if NVD or Apache confirms RCE is exploitable in the wild, if affected Apache instances process PII or PHI (triggering breach notification assessment under HIPAA or applicable state law), or if the organization cannot patch within 24 hours and HTTP/2 cannot be disabled as a containment measure.

Recovery Notes	After patching and re-enabling HTTP/2, monitor Apache error.log continuously for a minimum of 72 hours for recurrence of segmentation fault or double-free indicators in the http2 worker context — a clean window post-patch confirms the vulnerable code path is resolved. Verify that cPanel-managed environments received the security update to the correct EasyApache-bundled mod_http2 version, not just the system Apache package, as these can be versioned independently. If NVD confirms RCE exploitability for CVE-2026-23918 after your remediation, initiate a retrospective review of Apache access logs and any core dumps from the pre-patch window to determine whether exploitation produced a web shell, reverse connection, or unauthorized process execution beyond the confirmed DoS condition.
Forensic Artifacts	Apache error.log entries containing 'child pid exit signal Segmentation fault' or 'double free' in the AH-prefixed http2 module log lines — direct indicator of the CVE-2026-23918 double-free condition being triggered in the HTTP/2 worker process. | Apache core dump files (location configured via CoreDumpDirectory in httpd.conf, defaulting to /etc/apache2/ or /tmp/) generated by HTTP/2 worker process crashes — these contain memory state at the moment of the double-free and are the primary forensic artifact for determining whether exploitation progressed beyond DoS. | Apache access.log entries with HTTP/2.0 protocol field combined with elevated RST or 5xx response codes from the same source IP in rapid succession — indicative of an attacker fuzzing or replaying the malformed HTTP/2 frame sequence that triggers the CVE-2026-23918 memory corruption. | Pre-patch SHA-256 hash and file metadata of /usr/lib/apache2/modules/mod_http2.so (or equivalent path) — establishes the vulnerable binary baseline and confirms whether the patched module was correctly deployed, per NIST SI-7 (Software, Firmware, and Information Integrity). | WAF or network IDS/IPS logs filtered for HTTP/2 HEADERS or CONTINUATION frame anomalies (oversized payloads, malformed pseudo-headers, or SETTINGS frame floods) targeting the affected Apache server's IP during the pre-patch window — network-layer evidence of exploit delivery attempts against the HTTP/2 module vulnerability.

Per-Action IR Details

Step 1: Containment — Identify all Apache HTTP Server instances in your environment with HTTP/2 enabled (check Apache config for 'Protocols h2' or 'h2c' directives). If patching cannot begin immediately, consider temporarily disabling HTTP/2 on externally facing servers by removing 'h2' from the Protocols directive and restarting Apache. Confirm affected version range from the CVE record at cve.org or the Apache Security Advisory before scoping containment.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run `grep -r 'Protocols' /etc/apache2/ /etc/httpd/` (Linux) or `findstr /s /i 'Protocols' C:\Apache24\conf\` (Windows) across all known Apache config paths to enumerate h2/h2c directives. For a 2-person team without a CMDB, cross-reference active listening services via `ss -tlnp | grep httpd` or `netstat -tlnp | grep apache` and confirm HTTP/2 negotiation with `curl -I --http2 https://` — a response advertising 'h2' in the Alt-Svc or via HTTP/2 protocol confirms exposure. To disable HTTP/2 without a full restart window, set `Protocols http/1.1` in the VirtualHost block and reload with `apachectl graceful`.

Evidence: Before disabling HTTP/2, capture the current Apache configuration state: copy all httpd.conf, apache2.conf, and VirtualHost config files under /etc/apache2/sites-enabled/ or /etc/httpd/conf.d/ to a read-only forensic staging directory. Record the running Apache version (`httpd -v` or `apache2 -v`) and loaded modules (`httpd -M | grep http2`) to establish baseline scope for the CVE-2026-23918 version check. Preserve a snapshot of currently open network connections (`ss -tnp`) to document any suspicious long-lived or half-open HTTP/2 connections that may indicate pre-patch exploitation attempts.

Step 2: Detection — Query asset inventory and CMDB for Apache HTTP Server deployments. Check web server access and error logs for anomalous HTTP/2 connection patterns, repeated connection resets, or segmentation fault entries in Apache error logs (error.log). Review WAF and IDS/IPS logs for unusual traffic volumes to HTTP/2 endpoints. No confirmed IOC signatures are available at time of data capture.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Parse Apache error.log for segfault and double-free indicators using: `grep -E '(segfault|double free|corrupted|AH[0-9]+.*h2|child pid.*exit signal Segmentation)' /var/log/apache2/error.log /var/log/httpd/error_log`. For HTTP/2 connection anomalies in access.log, isolate HTTP/2 requests (logged as protocol 'HTTP/2.0') with high reset or 4xx/5xx ratios: `awk '$7 ~ /HTTP\/2/ && ($9 ~ /^[45]/)' /var/log/apache2/access.log | sort | uniq -c | sort -rn`. Deploy a Sigma rule targeting Apache process crashes via systemd journal: `journalctl -u apache2 --since '24h ago' | grep -i 'segfault\|core dump\|killed'`. If Wireshark or tcpdump is available, capture HTTP/2 traffic on port 443/80 and filter for RST_STREAM frames with error code 0x2 (INTERNAL_ERROR) which may indicate server-side memory corruption responses.

Evidence: Collect Apache error.log and access.log from all HTTP/2-enabled vhosts covering at minimum the 30 days prior to advisory publication — CVE-2026-23918 involves a double-free in the HTTP/2 module, meaning exploitation attempts would manifest as segmentation fault entries (e.g., 'AH00052: child pid XXXX exit signal Segmentation fault') in error.log. Capture any core dump files generated by Apache worker processes (typically in /etc/apache2/, /tmp/, or as configured by CoreDumpDirectory in httpd.conf) as these may contain memory state at the time of the double-free trigger. Preserve WAF logs filtering on HTTP/2 CONTINUATION or HEADERS frame floods, which are common vectors for memory corruption in HTTP/2 implementations.

Step 3: Eradication — Apply the Apache Software Foundation's official patch for CVE-2026-23918. Retrieve the authoritative patch and affected version range from httpd.apache.org/security/vulnerabilities_24.html (verify URL resolves) or the official CVE record. For cPanel-managed environments, apply the cPanel security update per the advisory at support.cpanel.net/hc/en-us/articles/40229402602519-Security-CVE-2026-23918.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For package-managed systems, apply the patched Apache version via: `apt-get update && apt-get install --only-upgrade apache2` (Debian/Ubuntu) or `yum update httpd` (RHEL/CentOS). Verify the installed version post-patch with `apache2 -v` or `httpd -v` and confirm it matches the fixed version listed in the Apache security advisory. For cPanel environments without direct shell access, navigate to WHM > cPanel Store > Security Advisor or run `/scripts/upcp --force` to pull the security update. After patching, verify the mod_http2 shared object is replaced: `md5sum /usr/lib/apache2/modules/mod_http2.so` — compare against the vendor-published checksum if available, per NIST SI-7 (Software, Firmware, and Information Integrity). For source-compiled Apache installs, rebuild from the patched source tarball and verify with `sha256sum` against the ASF-published digest before installation.

Evidence: Before applying the patch, capture the SHA-256 hash and file metadata of the existing mod_http2.so (`sha256sum /usr/lib/apache2/modules/mod_http2.so; stat /usr/lib/apache2/modules/mod_http2.so`) to establish a pre-patch baseline for the vulnerable binary. If any core dumps from Apache worker processes exist (see Step 2), preserve them now — they are volatile artifacts specific to the double-free condition in CVE-2026-23918 and will not be regeneratable post-patch. For cPanel environments, capture the pre-patch EasyApache profile (`/etc/cpanel/ea4/profiles/`) to document the exact Apache and mod_http2 build configuration before the security update overwrites it.

Step 4: Recovery — After patching, confirm the Apache service starts without error and HTTP/2 functionality operates normally. Review error logs for any residual crash indicators. Retest externally facing services with an HTTP/2 client to confirm normal response. If HTTP/2 was temporarily disabled as a containment measure, re-enable only after the patch is applied and verified.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Perform a structured HTTP/2 functional verification using `curl -v --http2 https:///` — confirm the response shows 'Using HTTP2, server supports HTTP multiplexing' and returns HTTP 200 without connection reset. Monitor Apache error.log in real-time for 15 minutes post-re-enablement: `tail -f /var/log/apache2/error.log | grep -E '(h2|http2|segfault|AH0)'`. For a zero-budget smoke test of HTTP/2 stability under load, use `ab -n 1000 -c 50 -r https:///` (Apache Bench, included with apache2-utils) and confirm no worker crashes appear in error.log during the run. If HTTP/2 was disabled as a containment measure, re-enable by restoring 'Protocols h2 http/1.1' to the VirtualHost block and issuing `apachectl configtest && apachectl graceful` — confirm no syntax errors before the graceful reload.

Evidence: After patching and re-enabling HTTP/2, capture a clean post-patch baseline of Apache error.log and the running module list (`httpd -M | grep http2`) to document the restored, non-vulnerable state. Record the exact timestamp of patch application and HTTP/2 re-enablement in the incident timeline — this establishes the remediation window boundary for any post-patch anomaly investigation. Preserve the output of `apache2ctl status` or `server-status` (if mod_status is enabled and restricted) immediately after recovery to document clean worker process state, contrasting against any worker pid segfault entries captured in Step 2.

Step 5: Post-Incident — Review your patch SLA against the time elapsed between disclosure and remediation for this CVE. Assess whether HTTP/2-enabled Apache instances are included in your external attack surface inventory. Evaluate whether your WAF or IPS has signatures covering malformed HTTP/2 request patterns as a compensating control for future HTTP/2-layer vulnerabilities.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Measure patch SLA by diffing the CVE publication timestamp against the patch application timestamp recorded in Step 4 — document this in the incident record to feed NIST IR-8 (Incident Response Plan) review cycles. To assess HTTP/2 attack surface coverage, run `nmap -p 80,443 --script http2-check ` or use `curl -I --http2 https://` in a scripted sweep across all externally-routable IPs to identify any Apache instances missed in initial scoping. For compensating WAF coverage without a commercial product, deploy the OWASP ModSecurity Core Rule Set (CRS) HTTP/2-relevant rules — specifically SecRule targeting oversized HEADERS frames and CONTINUATION frame floods — as a detection layer for future HTTP/2 memory-corruption class vulnerabilities in Apache.

Evidence: Compile the full incident artifact package for lessons-learned review: pre-patch mod_http2.so hash, error.log excerpts showing any crash indicators, patch application timestamp, post-patch verification output, and the scope of Apache instances identified. Document whether any Apache instances were discovered during this event that were not in the existing asset inventory — gaps here represent a finding against CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) that must feed back into the vulnerability management program. Retain all logs for a minimum period consistent with NIST AU-11 (Audit Record Retention) and your organizational retention policy, as post-incident NVD confirmation of RCE potential for CVE-2026-23918 could elevate this to a reportable incident requiring retrospective log review.

Detection Guidance

No confirmed exploitation signatures or IOC patterns are available in the current dataset for CVE-2026-23918. Detection should focus on behavioral indicators: (1) Apache error logs, search for segfault, double free, or heap corruption messages in /var/log/apache2/error.log or equivalent; (2) HTTP/2 connection anomalies, elevated connection reset rates or abnormal GOAWAY frame counts in access logs; (3) Process monitoring, unexpected Apache worker process crashes or restarts (systemd journal: 'journalctl -u apache2' for segfault events); (4) Network layer, traffic spikes targeting port 443/80 with HTTP/2 upgrade headers from single or distributed sources (correlate with T1499 DoS pattern). Until NVD publishes confirmed technical details and security vendors release detection signatures, these behavioral indicators represent the available detection surface. Recheck NVD and your EDR/IPS vendor for updated detection signatures within 48 hours of patch release, and refresh again after deploying patches to confirm signature updates are available for forensic validation.

Framework Mappings

MITRE-ATTACK

- **T1499** — Endpoint Denial of Service
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499	Endpoint Denial of Service	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://thehackernews.com/2026/05/critical-apache-http2-flaw-cve-20...	T3
(consolidated)	https://securityaffairs.com/191759/security/apache-fixes-critical-h...	T3
CVE-2026-23918 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-23918	T3
Critical Apache HTTP/2 Flaw (CVE-2026-23918) Enables DoS and ...	https://www.reddit.com/r/SecOpsDaily/comments/1t4lkr3/critical_apac...	T3
Security: CVE-2026-23918 - cPanel Support	https://support.cpanel.net/hc/en-us/articles/40229402602519-Securit...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-23918	T1

Generated 2026-05-06 09:04 UTC by TJS Security Command Center