INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-02 07:14 UTC

Adobe Discloses Nine Vulnerabilities Including Seven CVSS 10.0 Flaws in ColdFusion and Campaign Classic

CVE VULNERABILITY | CRITICAL | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0379
Type	CVE Vulnerability
CVE ID	CVE-2026-48276, CVE-2026-48277, CVE-2026-48281, CVE-2026-48282, CVE-2026-48283, CVE-2026-48286, CVE-2026-48313, CVE-2026-48315, CVE-2026-48316
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0092 (56th percentile)
Affected Products	Adobe ColdFusion 2023 (pre-Update 21), Adobe ColdFusion 2025 (pre-Update 10), Adobe Campaign Classic v7 build 9396 and earlier (Windows and Linux, on-premise deployments only)
Published	2026-07-01T11:25:46
Discovery Source	Rss

Executive Summary

On July 1, 2026, Adobe disclosed nine vulnerabilities across ColdFusion 2023/2025 and on-premise Campaign Classic v7, with seven of the nine carrying CVSS 10.0 scores, all enabling arbitrary code execution. Organizations running unpatched, on-premise deployments of these products face complete system compromise if exploitation occurs, including potential data exfiltration, ransomware staging, and service disruption. Adobe confirmed no active exploitation at time of disclosure, but the breadth of vulnerability classes and maximum severity scores warrant immediate patch prioritization.

Technical Analysis

Adobe disclosed nine CVEs on July 1, 2026, affecting ColdFusion 2023 (pre-Update 21), ColdFusion 2025 (pre-Update 10), and Campaign Classic v7 build 9396 and earlier (on-premise, Windows and Linux only). Seven CVEs - CVE-2026-48276, CVE-2026-48277, CVE-2026-48281, CVE-2026-48282, CVE-2026-48283, CVE-2026-48286, and CVE-2026-48313 - carry CVSS 10.0 scores and enable arbitrary code execution. CVE-2026-48315 and CVE-2026-48316 complete the set. The CWE profile spans four distinct weakness classes: unrestricted file upload (CWE-434), improper input validation (CWE-20), path traversal (CWE-22), and

incorrect authorization (CWE-863). Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1505.003 (Web Shell), T1068 (Exploitation for Privilege Escalation), and T1083 (File and Directory Discovery). Cloud-hosted Campaign Classic instances are not affected. EPSS score is 0.00917 (55.8th percentile) as of data capture; no CISA KEV listing confirmed at time of disclosure. Per source data, NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-48276) and the Adobe Security Advisory (https://helpx.adobe.com/security/products.html) are the authoritative references for per-CVE CVSS vectors and CWE mappings.

Action Checklist

1. Step 1: Containment. Immediately restrict inbound access to all on-premise instances of ColdFusion 2023 (pre-Update 21), ColdFusion 2025 (pre-Update 10), and Campaign Classic v7 build 9396 and earlier to known administrative IP ranges only; block all direct internet-facing access until patches are applied. Use perimeter firewall or WAF rules to enforce this restriction (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Review web server and application logs on ColdFusion and Campaign Classic hosts for anomalous file upload activity (CWE-434), unexpected .cfm/.jsp/.php file creation in web-accessible directories (T1505.003), and path traversal patterns (../ sequences in request URIs). Check for new or modified files in ColdFusion WEB-INF and wwwroot directories. Enable or verify audit logging is active per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation); use CIS 8.2 (Collect Audit Logs) as the baseline logging standard. Monitor system files for unauthorized modifications using file integrity monitoring tools (NIST SI-7, Information System Monitoring).
3. Step 3: Eradication. Apply Adobe's patches immediately: upgrade ColdFusion 2023 to Update 21 or later and ColdFusion 2025 to Update 10 or later per the Adobe Security Advisory (https://helpx.adobe.com/security/products.html). Upgrade Campaign Classic v7 to a build later than 9396 for on-premise Windows and Linux deployments. Confirm patch versions against the Adobe advisory; do not rely solely on automated patch tools without verification. Rotate service account credentials for any accounts with access to the patched systems, given the incorrect authorization weakness (CWE-863). Enforce CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) going forward.
4. Step 4: Recovery. After patching, verify running version numbers against Adobe's confirmed fixed-version list. Audit web-accessible directories on ColdFusion and Campaign Classic servers for any web shells or unauthorized uploaded files deposited prior to patching using file integrity monitoring. Restore from known-good backups if unauthorized file creation is detected. Re-enable full external access only after patch verification is complete and no indicators of compromise are found. Monitor application and OS logs for 72 hours post-patch for residual anomalous activity (NIST AU-6, Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Evaluate whether ColdFusion and Campaign Classic deployments require internet exposure; restrict to internal or VPN-only access where operationally feasible (NIST AC-17, Remote Access). Review file upload handling controls and input validation configurations against CWE-434 and CWE-20 mitigations. Assess whether Adobe's patching cadence requires adjustments to your patch management SLA. Document this event in your vulnerability management program and update remediation SLAs for CVSS 10.0 findings (CIS 7.1, Establish and Maintain a Vulnerability Management Process; CIS 7.2, Establish and Maintain a Remediation Process). Review and restrict user account permissions to limit which accounts can upload files or modify web-accessible directories on application

servers (NIST AC-2, Account Management).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and breach notification counsel immediately if web shell artifacts, unauthorized file creation, or attacker-controlled process execution are confirmed on any ColdFusion or Campaign Classic host that stores, processes, or transmits PII, PHI, or payment card data — particularly given the seven CVSS 10.0 arbitrary code execution flaws and the potential for ransomware staging and data exfiltration noted in the advisory.
Recovery Notes	Before re-enabling external access to any ColdFusion 2023/2025 or Campaign Classic v7 host, confirm the installed version explicitly against Adobe's fixed-version list (ColdFusion 2023 Update 21+, ColdFusion 2025 Update 10+, Campaign Classic build > 9396) — do not infer patch status from automated tools alone. Conduct a full web shell sweep of all ColdFusion wwwroot and WEB-INF directories and Campaign Classic web-accessible paths using file integrity comparison and YARA scanning before returning hosts to production. Maintain heightened log monitoring for 72 hours post-recovery, specifically watching for ColdFusion JVM or nlserver spawning unexpected child processes, which would indicate a persistent backdoor survived eradication.
Forensic Artifacts	ColdFusion access log ({CF_HOME}/cfusion/logs/access.log and server.log): POST requests to /CFIDE/, /CFFileServlet/, or arbitrary .cfm endpoints with large request bodies, path traversal sequences (../, %2e%2e%2f, %252e), or responses returning file paths — direct evidence of CVE-2026-48276/48277 file upload exploitation attempts. | Windows Security Event ID 4688 (Process Creation) with parent process coldfusion.exe or java.exe spawning cmd.exe, powershell.exe, wscript.exe, or net.exe — the canonical process tree signature of ColdFusion arbitrary code execution exploitation (relevant to all seven CVSS 10.0 RCE CVEs in this advisory). | Filesystem timestamps and hashes for all .cfm, .jsp, .php files in ColdFusion wwwroot ({CF_HOME}/cfusion/wwwroot/) and WEB-INF directories: files created or modified after the Adobe disclosure date (July 1, 2026) with no corresponding legitimate deployment record are high-confidence web shell indicators for CVE-2026-48313/48315/48316. | Campaign Classic nlserver process logs (/var/log/nlserver/ on Linux, Windows Event Log for nlserver service on Windows) and network connections from the nlserver process (captured via `netstat -ano` filtered on nlserver PID): unexpected outbound connections to non-Adobe, non-organizational IPs from the Campaign Classic process indicate post-exploitation C2 activity following exploitation of the Campaign Classic CVEs. | RAM image analyzed for JVM heap artifacts: on a ColdFusion host, memory forensics (WinPmem/LiME + Volatility3) targeting the java.exe process heap can recover deserialization payload fragments, injected shellcode, and in-memory credential material that would not appear in any on-disk log — critical given that several of these CVEs involve incorrect authorization and deserialization weaknesses that operate entirely in memory prior to writing a web shell.

Per-Action IR Details

Step 1: Containment — Immediately identify all on-premise instances of ColdFusion 2023 (pre-Update 21), ColdFusion 2025 (pre-Update 10), and Campaign Classic v7 build 9396 and earlier. Block direct internet access to these hosts at the perimeter firewall or WAF until patches are applied. Restrict inbound connections to known administrative IP ranges (NIST AC-4 — Information Flow Enforcement; CIS 4.4 — Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run `netstat -ano` (Windows) or `ss -tlnp` (Linux) on each suspected ColdFusion or Campaign Classic host to enumerate listening ports (default ColdFusion HTTP: 8500, HTTPS: 8443; Campaign Classic MTA: 4022, 8080). Add deny-all inbound rules for those ports on the host firewall using `netsh advfirewall firewall add rule` (Windows) or `iptables -I INPUT -p tcp --dport 8500 -j DROP` (Linux) until perimeter rules are confirmed. Enumerate all ColdFusion instances with `wmic product where 'name like "Adobe ColdFusion%"' get name,version` (Windows) or `rpm -qa | grep -i coldfusion` (Linux).

Evidence: Before blocking network access — which destroys live connection state — capture: (1) active network connections and listening services via `netstat -ano > netstat_pre_block.txt` or `ss -tlnp > ss_pre_block.txt`; (2) all current established sessions to ColdFusion ports (8500/8443) and Campaign Classic ports (4022/8080/443) to identify any active attacker sessions already in progress; (3) running process list via `tasklist /v > proclist_pre_block.txt` (Windows) or `ps auxf > proclist_pre_block.txt` (Linux) to identify any child processes spawned by the ColdFusion JVM (coldfusion.exe / java process) or Campaign Classic nlserver process that may indicate active exploitation before containment action severs the connection.

Step 2: Detection — Review web server and application logs on ColdFusion and Campaign Classic hosts for anomalous file upload activity (CWE-434), unexpected .cfm/.jsp/.php file creation in web-accessible directories (T1505.003), and path traversal patterns (../ sequences in request URIs). Check for new or modified files in ColdFusion WEB-INF and wwwroot directories. Enable or verify audit logging is active per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation); use CIS 8.2 (Collect Audit Logs) as the baseline logging standard. Apply D3-SFA (System File Analysis) to monitor for unauthorized modifications to system executables and configuration files on affected hosts.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: On ColdFusion hosts, run `Get-ChildItem -Path 'C:\ColdFusion2023\cfusion\wwwroot' -Recurse -Include *.cfm,*.jsp,*.php,*.asp -NewerThan (Get-Date).AddDays(-7) | Select FullName,CreationTime,LastWriteTime` to identify recently created web-accessible files. On Linux Campaign Classic hosts: `find /var/www/ /opt/campaign/ -name '*.php' -o -name '*.jsp' -newer /tmp/baseline_ref -ls 2>/dev/null`. Parse ColdFusion access logs at `{CF_HOME}/cfusion/logs/access.log` using `grep -E '(\.\./|%2e%2e|%252e|file=|upload|PUT )' access.log` to surface path traversal and upload attempts. Deploy Sysmon with Event ID 11 (FileCreate) filtering on `.cfm`, `.jsp`, `.php` extensions in web root directories to catch web shell drops in real time.

Evidence: This is a detection/analysis step — it does not alter live host state. However, if active exploitation indicators are found during this review (e.g., a newly created .cfm web shell or a ColdFusion JVM spawning cmd.exe), treat the host as actively compromised and immediately capture RAM (via WinPmem or LiME kernel module) and volatile process/network state before proceeding to containment. Specific artifacts to examine: ColdFusion request log at `{CF_HOME}/cfusion/logs/server.log` and `application.log` for Java exceptions indicating deserialization or file write errors; IIS/Apache access logs for POST requests to `/CFIDE/`, `/CFFileServlet/`, or any `.cfm` endpoint with unusually large request bodies (potential file upload payloads); Windows Security Event ID 4688 (Process Creation) filtering on `cmd.exe`, `powershell.exe`, `wscript.exe`, or `cscript.exe` with a parent process of `coldfusion.exe` or `java.exe`; Campaign Classic nlserver log at `/var/log/nlserver/` for unexpected subprocess execution.

Step 3: Eradication — Apply Adobe's patches immediately: upgrade ColdFusion 2023 to Update 21 or later and ColdFusion 2025 to Update 10 or later per the Adobe Security Advisory (https://helpx.adobe.com/security/products.html). Upgrade Campaign Classic v7 to a build later than 9396 for on-premise Windows and Linux deployments. Confirm patch versions against the Adobe advisory; do not rely solely on automated patch tools without verification. Apply D3-CRO (Credential Rotation) for any service accounts with access to the patched systems, given the incorrect authorization weakness (CWE-863). Enforce

CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) going forward.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before patching, verify no web shells or unauthorized files exist in ColdFusion web roots — patching over an active web shell leaves the backdoor intact. Use `certutil -hashfile ColdFusion_2023_WWEJ_win.exe SHA256` (Windows) or `sha256sum` (Linux) to verify the Adobe patch installer hash against the value published in the Adobe Security Advisory before executing. After applying ColdFusion Update 21, confirm the installed update level via `{CF_HOME}/cfusion/bin/cf-cli.bat version` or inspect `{CF_HOME}/cfusion/lib/neo-runtime.xml` for the version string. For Campaign Classic, verify the build number post-upgrade via the server console `nlserver monitor` command. Rotate all ColdFusion data source passwords, CFIDE administrator passwords, and Campaign Classic operator account credentials using your password manager or `net user` / `passwd` commands immediately after patching.

Evidence: Patching permanently alters the vulnerable binary — this is an eradication action that modifies live system state. Before applying any patch: (1) acquire a full RAM image using WinPmem (`winpmem_mini_x64.exe --output ram.aff4`) or LiME (`insmod lime.ko path=/mnt/evidence/ram.lime format=lime`) to preserve any in-memory attacker artifacts (injected shellcode, stolen credentials in JVM heap, active C2 beacon state); (2) snapshot all running processes and their loaded DLLs/shared libraries (`tasklist /m > loaded_modules.txt` or `lsof -p $(pgrep -f coldfusion) > loaded_libs.txt`); (3) export current ColdFusion service account tokens and active Windows logon sessions via `whoami /all > session_context.txt`; (4) image or hash all files in `{CF_HOME}/cfusion/wwwroot/`, `WEB-INF/`, and Campaign Classic `/conf/` directories before the patch modifies them, to preserve the pre-patch filesystem state for forensic comparison.

Step 4: Recovery — After patching, verify running version numbers against Adobe's confirmed fixed-version list. Audit web-accessible directories on ColdFusion and Campaign Classic servers for any web shells or unauthorized uploaded files deposited prior to patching (D3-SFA). Restore from known-good backups if unauthorized file creation is detected. Re-enable full external access only after patch verification is complete and no indicators of compromise are found. Monitor application and OS logs for 72 hours post-patch for residual anomalous activity (NIST AU-6 — Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Perform a file integrity baseline comparison: hash all files in ColdFusion wwwroot and WEB-INF directories post-patch using `Get-FileHash -Algorithm SHA256 -Path 'C:\ColdFusion2023\cfusion\wwwroot\*' -Recurse | Export-Csv hashes_post_patch.csv` and diff against a known-good baseline or the Adobe-distributed file manifest. Deploy a YARA rule scanning for common ColdFusion web shell signatures (e.g., CFM files containing `cfexecute`, `createObject('java')`, or `Runtime.getRuntime().exec()`) across all web-accessible directories: `yara -r coldfusion_webshell.yar /opt/coldfusion/wwwroot/`. For Campaign Classic, verify integrity of nlserver binary via `md5sum /usr/local/neolane/nl6/bin/nlserver` against the Adobe-published binary hash. Monitor ColdFusion `server.log` and Windows Event ID 4688 during the 72-hour watch period for any process tree anomalies (java.exe or nlserver spawning shells).

Evidence: Recovery actions (re-enabling external access, restoring from backup) do not destroy volatile evidence since eradication is already complete at this phase. However, during the web shell audit, if a live web shell is discovered that was not previously detected, treat the host as not yet eradicated — revert to containment, capture RAM and active process state immediately before removing the shell, as a resident shell may have active C2 connections or injected threads that are only visible in memory. Document all file hashes, modification timestamps, and directory listings from the post-patch audit as recovery verification evidence for the incident record.

Step 5: Post-Incident — Evaluate whether ColdFusion and Campaign Classic deployments require internet exposure; restrict to internal or VPN-only access where operationally feasible (NIST AC-17 — Remote

Access). Review file upload handling controls and input validation configurations against CWE-434 and CWE-20 mitigations. Assess whether Adobe's announced twice-monthly patching cadence requires adjustments to your patch management SLA. Document this event in your vulnerability management program and update remediation SLAs for CVSS 10.0 findings (CIS 7.1 — Establish and Maintain a Vulnerability Management Process; CIS 7.2 — Establish and Maintain a Remediation Process). Apply D3-UAP (User Account Permissions) review to limit which accounts can upload files or modify web-accessible directories on application servers.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AC-6 (Least Privilege)

Compensating: Document the gap between Adobe's July 1, 2026 disclosure date and your patch completion date as your mean-time-to-remediate (MTTR) for CVSS 10.0 findings — if that gap exceeded 24 hours for internet-exposed ColdFusion instances, your patch SLA requires revision. Configure osquery on ColdFusion and Campaign Classic hosts with a scheduled query against `file` table monitoring `{CF_HOME}/cfusion/wwwroot/` and Campaign Classic `/var/www/` for new file creation events, and schedule it to run every 15 minutes as a persistent post-recovery tripwire: `SELECT filename, path, mtime FROM file WHERE path LIKE '/opt/coldfusion/wwwroot/%' AND mtime > (strftime('%s','now') - 900);`. Submit IOCs (any discovered web shell hashes, anomalous source IPs from access logs) to CISA's AIS program or your sector ISAC to support community detection.

Evidence: This phase produces program-level documentation rather than volatile forensic evidence. Collect and preserve as incident record artifacts: the complete ColdFusion access log archive covering the window from Adobe's disclosure (July 1, 2026) back 30 days (to establish a pre-disclosure baseline and detect any pre-patch exploitation attempts); the pre- and post-patch file hash manifests from Step 4; all firewall rule change records from Step 1 containment; and patch verification outputs from Steps 3 and 4. These artifacts support both internal lessons-learned and any external regulatory breach notification assessment if PII or PHI was accessible to the ColdFusion or Campaign Classic application tier.

Detection Guidance

Focus detection efforts on ColdFusion and on-premise Campaign Classic v7 hosts. Key indicators to hunt: (1) HTTP POST requests to ColdFusion endpoints containing path traversal sequences (../, %2e%2e%2f, %252e) in URI parameters; correlate web access logs against known-good URI patterns. (2) New or modified files with executable extensions (.cfm, .cfc, .jsp, .php, .exe, .sh) in web-accessible directories created outside of authorized change windows; map to T1505.003 (Web Shell) and CWE-434. (3) Processes spawned by the ColdFusion or Campaign Classic service account (e.g., coldfusion.exe, java.exe on Windows; java on Linux) that invoke system shells (cmd.exe, powershell.exe, /bin/bash, /bin/sh); map to T1059. (4) Authorization errors or unexpected access grants in ColdFusion administrator and Campaign Classic operator logs; map to CWE-863. (5) Directory listing or file enumeration activity from the application process; map to T1083. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and NIST SI-7 (Information System Monitoring) as the detection framework. No confirmed IOCs were present in the source data at time of disclosure; hunting should rely on behavioral and structural indicators above.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

- **T1083** — File and Directory Discovery
- **T1068** — Exploitation for Privilege Escalation
- **T1059** — Command and Scripting Interpreter
- **T1505.003** — Web Shell

NIST-800-53R5

- **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
- **AC-6** — Least Privilege
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-2** — Baseline Configuration
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A03:2021** — Injection
- **A04:2021** — Insecure Design

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **6.1** — Establish an Access Granting Process
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1083	File and Directory Discovery	Discovery
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution
T1505.003	Web Shell	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/adobe-patches-7-cvss-100-flaws-in...	T2
CVE-2026-48276 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-48276	T3
CVE-2026-48276 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-48276	T1
Adobe Patches Critical ColdFusion, Campaign Classic Vulnerabilities	https://radar.offseq.com/threat/adobe-patches-critical-coldfusion-c...	T3
May 2026 CVE Landscape - Recorded Future	https://www.recordedfuture.com/blog/may-2026-cve-landscape	T1
Adobe Security Advisory	https://helpx.adobe.com/security/products.html	T1

Generated 2026-07-02 07:14 UTC by TJS Security Command Center