INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:05 UTC

Delta ASDA-Soft Stack-Based Buffer Overflow Enables Arbitrary Code Execution (CVE-2026-5726)

CVE VULNERABILITY | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CVE-2026-0048
Type	CVE Vulnerability
CVE ID	CVE-2026-5726
Severity	HIGH
CVSS Base Score	7.8
EPSS Score	0.0001 (0th percentile)
Affected Products	Delta Electronics ASDA-Soft configuration software (versions prior to v7.2.6.0)
Published	2026-04-16
Discovery Source	Gemini

Executive Summary

A stack-based buffer overflow in Delta Electronics ASDA-Soft configuration software allows an attacker to execute arbitrary code on any engineering workstation running an unpatched version. The vulnerability affects industrial environments using Delta ASDA-series servo drives, where compromise of a configuration host could disrupt or manipulate connected operational technology. A patch is available in version 7.2.6.0; organizations running earlier versions should prioritize patching within 30 days.

Technical Analysis

CVE-2026-5726 is a stack-based buffer overflow (CWE-121) in Delta Electronics ASDA-Soft, the Windows-based configuration utility for ASDA-series servo drives. Affected versions: all releases prior to v7.2.6.0. CVSS 3.x base score: 7.8 (High). Attack vector requires local access; exploitation is most likely achieved by convincing a technician or engineer to open a maliciously crafted project or configuration file (MITRE T1203: Exploitation for Client Execution; T1204.002: Malicious File). A successful exploit overwrites stack memory and may enable arbitrary code execution in the context of the logged-in user. No in-the-wild exploitation has been confirmed; EPSS score is 0.005% (percentile 0.257%), indicating currently low exploitation probability. CISA published ICS advisory ICSA-26-106-02 on April 16, 2026. A prior advisory (ICSA-25-296-04) references the same product, indicating a pattern of buffer overflow findings in this software line. Patch: upgrade to ASDA-Soft v7.2.6.0 or later per Delta Electronics and CISA guidance.

Action Checklist

1. Step 1: Containment. Immediately inventory all engineering workstations running Delta ASDA-Soft versions prior to v7.2.6.0. Block file transfers (USB, email attachments, network shares) to those hosts until patched. Block untrusted project files from reaching ASDA-Soft workstations via network segmentation or endpoint controls.
2. Step 2: Detection. Query endpoint management or asset inventory tools for installed versions of ASDA-Soft (look for file version metadata on ASDA-Soft executables below v7.2.6.0). Review application event logs on affected workstations for unexpected crashes or access violations in the ASDA-Soft process, which may indicate failed exploitation attempts. No public IOCs (hashes, IPs, domains) are currently associated with active exploitation of this CVE.
3. Step 3: Eradication. Upgrade ASDA-Soft to version 7.2.6.0 or later per CISA advisory ICSA-26-106-02 and Delta Electronics guidance. Obtain the patch directly from Delta Electronics' official support portal. Do not source installers from third-party sites.
4. Step 4: Recovery. After upgrading, verify the installed version matches v7.2.6.0 or later via the application's About menu or file properties. Confirm servo drive communications function normally post-upgrade. Monitor workstation process behavior for any anomalies in the days following patching.
5. Step 5: Post-Incident. Review the intake process for ASDA-Soft project files: establish a policy requiring that configuration files sourced externally (from vendors, contractors, or removable media) are validated before opening. Assess whether ASDA-Soft workstations have unnecessary privileges that would amplify code execution impact. Note that ICSA-25-296-04 indicates prior findings in this product line; schedule recurring review of Delta Electronics security advisories.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to OT/ICS security leadership and plant operations if any ASDA-Soft workstation exhibits evidence of successful code execution (child processes spawned from ASDASoft.exe, WER dumps showing controlled RIP/EIP hijack, or unexpected network connections from the workstation to non-Delta infrastructure), or if any workstation has direct network connectivity to ASDA-series servo drive controllers without an intervening firewall, as arbitrary code execution on a directly-connected engineering workstation could enable manipulation of servo drive parameters with physical consequences.
Recovery Notes	After patching to v7.2.6.0, perform a controlled functional test of ASDA-Soft communications with each connected ASDA-series servo drive by executing a read-back of axis configuration parameters and comparing against known-good baselines to confirm no unauthorized parameter changes occurred during the exposure window. Monitor ASDA-Soft workstations via Sysmon Event ID 1 for unexpected child process spawns for a minimum of 72 hours post-patch, as a threat actor who achieved pre-patch persistence may have installed a secondary payload (scheduled task, DLL side-load within the ASDA-Soft directory) that survives the application upgrade. Retain all pre-patch forensic artifacts (crash dumps, process baselines, registry snapshots) for a minimum of 90 days in a write-protected evidence store aligned with NIST AU-11 (Audit Record Retention) requirements.

Forensic Artifacts	Windows Error Reporting crash dumps for ASDASoft.exe at %LocalAppData%\CrashDumps\ and %ProgramData%\Microsoft\Windows\WER\ReportArchive\ — a stack-based buffer overflow that does not achieve controlled execution will produce an access violation (0xC0000005) dump containing the overflowed stack frame and any embedded shellcode; these are the primary artifact of failed exploitation. | Windows Application Event Log (Event ID 1000 and 1001) filtered on faulting application ASDASoft.exe — repeated crash entries in the days prior to patching indicate active exploitation attempts against the stack-based buffer overflow in CVE-2026-5726, even absent confirmed IOCs. | Sysmon Event ID 1 (Process Create) logs filtered on parent process ASDASoft.exe — any child process (cmd.exe, powershell.exe, mshta.exe, rundll32.exe) spawned by ASDA-Soft is a high-confidence indicator of successful arbitrary code execution via the buffer overflow. | ASDA-Soft recent files MRU registry key at HKCU\Software\Delta\ASDASoft\RecentFiles — enumerates all project files (.asd, .prj) opened on the workstation, identifying which externally-sourced configuration files were the potential delivery mechanism for a maliciously crafted buffer-overflow-triggering project file. | Pre- and post-patch SHA-256 file hash inventory of C:\Program Files\Delta\ASDA Soft\ — a threat actor who achieved code execution prior to patching may have trojanized a DLL within the ASDA-Soft installation directory (e.g., a side-loaded dependency); diffing pre-patch hashes against known-good v7.2.6.0 hashes from Delta Electronics identifies any tampered or injected files that survived the upgrade.

Per-Action IR Details

Step 1: Containment — Immediately inventory all engineering workstations running Delta ASDA-Soft versions prior to v7.2.6.0. Restrict file transfers (USB, email attachments, network shares) to those hosts until patched. Block untrusted project files from reaching ASDA-Soft workstations via network segmentation or endpoint controls.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run the following PowerShell on each candidate workstation to confirm version: `(Get-Item 'C:\Program Files\Delta\ASDA Soft\ASDASoft.exe').VersionInfo.FileVersion`. For USB blocking without EDR, use Windows Group Policy (Computer Configuration → Administrative Templates → System → Removable Storage Access → All Removable Storage Classes: Deny all access). For network share isolation, apply host-based Windows Firewall rules via netsh: `netsh advfirewall firewall add rule name='Block SMB ASDA-Soft Host' protocol=TCP dir=in localport=445 action=block`. Deploy these via a batch script pushed through any available RMM or manually per host.

Evidence: Before isolating, capture a snapshot of active network connections from the ASDA-Soft workstation using `netstat -ano > C:\IR\netstat_baseline.txt` and `Get-Process | Export-Csv C:\IR\process_baseline.csv` to establish a pre-containment baseline. Preserve Windows Security Event Log (EVTX) from `%SystemRoot%\System32\winevt\Logs\Security.evtx` and Application Event Log focused on events from the ASDA-Soft process. Note any recently accessed .asd or .prj project files in the MRU list at `HKCU\Software\Delta\ASDASoft\RecentFiles` — these are the most likely delivery vectors for a malicious buffer-overflow-triggering project file.

Step 2: Detection — Query endpoint management or asset inventory tools for installed versions of ASDA-Soft (look for file version metadata on ASDA-Soft executables below v7.2.6.0). Review application event logs on affected workstations for unexpected crashes or access violations in the ASDA-Soft process, which may indicate failed exploitation attempts. No public IOCs (hashes, IPs, domains) are currently associated with active exploitation of this CVE.

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 SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without an enterprise asset management tool, run the following PowerShell remotely across workstations to enumerate ASDA-Soft versions: `Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*' | Where-Object {$_.DisplayName -like '*ASDA*'} | Select-Object DisplayName, DisplayVersion, InstallLocation`. For crash detection without EDR, deploy Sysmon (Sysinternals) with Event ID 1 (Process Create) and Event ID 3 (Network Connection) filtering on `ASDASoft.exe`, and query Windows Application Event Log for Event ID 1000 (Application Error) with faulting application name `ASDASoft.exe` — a stack-based buffer overflow that fails to achieve code execution will typically produce a structured exception (access violation, 0xC0000005) logged here. Use: `Get-WinEvent -LogName Application | Where-Object {$_.Id -eq 1000 -and $_.Message -like '*ASDASoft*'}`.

Evidence: Pull Windows Application Event Log entries with Event ID 1000 (Application Crash) and Event ID 1001 (Windows Error Reporting) for `ASDASoft.exe` — a failed stack smash will fault here before controlled execution is achieved. Collect WER (Windows Error Reporting) crash dumps from `%LocalAppData%\CrashDumps\` or `%ProgramData%\Microsoft\Windows\WER\ReportArchive\` for any ASDA-Soft crash reports; these dumps may contain stack traces revealing the overflowed buffer and any shellcode precursor. Also review `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps` to confirm dump capture is enabled. Query Sysmon Event ID 1 for any child processes spawned by `ASDASoft.exe` (cmd.exe, powershell.exe, rundll32.exe), which would indicate successful code execution rather than a crash.

Step 3: Eradication — Upgrade ASDA-Soft to version 7.2.6.0 or later per CISA advisory ICSA-26-106-02 and Delta Electronics guidance. Obtain the patch directly from Delta Electronics' official support portal. Do not source installers from third-party sites.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-3 (Configuration Change Control), 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: Download the ASDA-Soft v7.2.6.0 installer exclusively from Delta Electronics' official support portal (https://www.deltaww.com/en-US/products/ServoMotors — verify the URL resolves to the Delta Electronics domain before downloading; this URL is provided for direction only and must be human-validated). Before executing the installer, verify its SHA-256 hash against the value published in ICSA-26-106-02 or the Delta Electronics advisory using: `Get-FileHash .\ASDASoft_Setup_v7.2.6.0.exe -Algorithm SHA256`. If the advisory does not publish a hash, contact Delta Electronics support directly to obtain one before deploying. Stage the verified installer on an internal file share and push via script to avoid repeated exposure to internet-sourced downloads.

Evidence: Before patching, preserve a forensic image or at minimum a file hash inventory of the current ASDA-Soft installation directory (typically `C:\Program Files\Delta\ASDA Soft\`) using `Get-ChildItem -Recurse | Get-FileHash | Export-Csv C:\IR\asdasoft_pre_patch_hashes.csv`. Capture the current Windows registry uninstall key for ASDA-Soft at `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\` to document the pre-patch version. If a prior crash was detected in Step 2, preserve the WER crash dumps before the patch installer overwrites any application files, as these dumps constitute primary forensic evidence of exploitation attempts.

Step 4: Recovery — After upgrading, verify the installed version matches v7.2.6.0 or later via the application's About menu or file properties. Confirm servo drive communications function normally post-upgrade. Monitor workstation process behavior for any anomalies in the days following patching.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Confirm patched version via PowerShell: `(Get-Item 'C:\Program Files\Delta\ASDA Soft\ASDASoft.exe').VersionInfo.FileVersion` — output must be `7.2.6.0` or higher. For post-patch behavioral monitoring without EDR, configure Sysmon to log Event ID 1 (Process Create) for `ASDASoft.exe` and alert on any child process spawns for a minimum of 72 hours post-patching; export daily with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -like '*ASDASoft*'} | Export-Csv C:\IR\asda_postpatch_procs.csv`. Verify ASDA-series servo drive communication by performing a controlled configuration read/write cycle and confirming expected axis response — involve OT/controls engineers for this validation step.

Evidence: Post-upgrade, collect a new file hash inventory of the ASDA-Soft installation directory using the same method as pre-patch to confirm all binaries have been replaced: `Get-ChildItem -Recurse | Get-FileHash | Export-Csv C:\IR\asdasoft_post_patch_hashes.csv`. Diff against the pre-patch inventory to confirm expected changes and detect any files that were not updated, which could indicate a partial or tampered installation. Retain the Windows Application Event Log for the 72-hour monitoring window to document the clean post-patch baseline.

Step 5: Post-Incident — Review the intake process for ASDA-Soft project files: establish a policy requiring that configuration files sourced externally (from vendors, contractors, or removable media) are validated before opening. Assess whether ASDA-Soft workstations have unnecessary privileges that would amplify code execution impact. Note that ICSA-25-296-04 indicates prior findings in this product line; schedule recurring review of Delta Electronics security advisories.

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 SI-10 (Information Input Validation), NIST AC-6 (Least Privilege), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Implement a project file quarantine workflow: any externally-sourced .asd or .prj file must be placed in a designated staging folder and scanned with ClamAV (`clamscan --max-filesize=50M --alert-exceeds-max=yes `) before an engineer opens it in ASDA-Soft. Additionally, run ASDA-Soft under a standard (non-admin) local user account — verify current token with `whoami /groups` and confirm absence of `BUILTIN\Administrators`; if present, create a dedicated low-privilege service account for ASDA-Soft operations. Establish a calendar reminder or RSS feed subscription for Delta Electronics security advisories (cross-reference CISA ICS advisories at https://www.cisa.gov/news-events/cybersecurity-advisories — human-validate this URL) to ensure ICSA notices for Delta products are reviewed within 5 business days of publication.

Evidence: Conduct a lessons-learned review documenting: (1) the date range during which vulnerable ASDA-Soft versions were in production, (2) whether any WER crash dumps from Step 2 were recovered and what they indicate about exploitation attempts, (3) the current privilege level under which ASDA-Soft runs on each workstation, and (4) the list of externally-sourced project files opened during the exposure window (recoverable from `HKCU\Software\Delta\ASDASoft\RecentFiles` and Windows Search index at `%ProgramData%\Microsoft\Search\Data\`). Cross-reference ICSA-25-296-04 findings against the current patch state to determine whether any prior vulnerability in this product line remains unremediated.

Detection Guidance

No confirmed IOCs (file hashes, network indicators, or behavioral signatures) are publicly associated with active exploitation of CVE-2026-5726 at this time. Detection focus should be on version enumeration and anomalous process behavior. Query endpoint agents or software inventory systems for ASDA-Soft installations below v7.2.6.0. On affected hosts, monitor Windows Event Logs for application crash events (Event ID 1000/1001 in

the Application log) tied to the ASDA-Soft process; repeated crashes may indicate exploitation attempts. If EDR is deployed on engineering workstations, create an alert for unexpected child processes spawned by ASDA-Soft or unusual memory access patterns. Given the file-based attack vector (T1204.002), also monitor for ASDA-Soft opening project files from unusual directories (temp folders, downloads, removable media) as a behavioral precursor indicator.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1204.002** — Malicious File

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SR-2** — Supply Chain Risk Management Plan

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
gemini	https://waterisac.org/articles/tlpclear-cisa-ics-advisories-additio...	T3
CVE-2026-5726 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-5726	T1
Delta Electronics ASDA-Soft - CISA	https://www.cisa.gov/news-events/ics-advisories/icsa-25-296-04	T1
CVE-2026-1361: ASDA-Soft Buffer Overflow Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-1361/	T3
Delta ASDA-Soft CVE-2026-5726 Buffer Overflow: Patch v7.2.6.0+	https://windowsforum.com/threads/delta-asda-soft-cve-2026-5726-buff...	T3

Generated 2026-04-17 14:05 UTC by TJS Security Command Center