INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:28 UTC

Adobe Acrobat and Reader Prototype Pollution Vulnerability Enables Arbitrary Code Execution (CVE-2026-34621)

CVE VULNERABILITY | HIGH | CVSS 8.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0033
Type	CVE Vulnerability
CVE ID	CVE-2026-34621
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0004 (11th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-04-27)
Affected Products	Adobe Acrobat and Reader (specific versions not confirmed from available data)
Published	2026-04-13
Discovery Source	Cisa Kev

Executive Summary

Adobe Acrobat and Reader contain an actively exploited prototype pollution vulnerability (CVE-2026-34621, CVSS 8.8) that allows attackers to execute arbitrary code on affected systems. CISA has confirmed active exploitation and added this to the Known Exploited Vulnerabilities catalog, with a remediation deadline of April 27, 2026. Any organization where employees open PDFs, including document workflows, contract review, or finance operations, is at direct risk of endpoint compromise.

Technical Analysis

CVE-2026-34621 is a prototype pollution vulnerability (CWE-1321) in Adobe Acrobat and Reader. Prototype pollution allows an attacker to inject properties into JavaScript object prototypes within the application's runtime, enabling logic manipulation that escalates to arbitrary code execution. MITRE ATT&CK techniques T1059.007 (JavaScript execution) and T1203 (exploitation for client execution) apply directly. CVSS base score is 8.8 (High). Specific affected versions have not been confirmed in available data, consult Adobe Security Bulletin APSB26-43 for the authoritative version matrix. Adobe has issued a patch; CISA KEV remediation deadline is 2026-04-27. EPSS score is 0.038% (11th percentile), which is low for a KEV-listed CVE, this discrepancy likely reflects the recency of the listing. KEV status supersedes EPSS for prioritization. Sources: CISA KEV (T1), NVD

(T1), Adobe Security Advisory (T1).

Action Checklist

1. Step 1: Containment, Identify all endpoints running Adobe Acrobat or Adobe Reader. Disable or restrict PDF opening in Acrobat/Reader via Group Policy or endpoint management until patching is confirmed. Prioritize internet-facing systems and endpoints used by finance, legal, and executive staff who routinely open external PDFs. Reference: Adobe APSB26-43.
2. Step 2: Detection, Search endpoint detection logs for suspicious child processes spawned by AcroRd32.exe or Acrobat.exe (e.g., cmd.exe, powershell.exe, wscript.exe). In SIEM, query for T1059.007 and T1203 process creation events parented to Adobe Reader or Acrobat. Review browser download logs for PDF files delivered from external sources in the past 30 days. No confirmed IOC hashes or C2 infrastructure are available from current sources.
3. Step 3: Eradication, Apply the patch detailed in Adobe Security Bulletin APSB26-43. Verify the installed version against the patched version matrix in that bulletin. If patching is not immediately possible, consider deploying Adobe Acrobat's Protected View mode (sandboxed rendering) as a temporary mitigation.
4. Step 4: Recovery, After patching, validate the installed version on all endpoints against the fixed version listed in APSB26-43. Re-enable PDF workflows. Monitor AcroRd32.exe and Acrobat.exe process trees for 14 days post-patch for any anomalous child process activity that could indicate a pre-patch compromise still persisting.
5. Step 5: Post-Incident, Review PDF handling policies: assess whether all staff require full Acrobat/Reader or whether a lighter, less attack-surface-heavy viewer is appropriate for general use. Evaluate whether application allowlisting or sandboxing is enforced for document viewer applications. Map this vulnerability to NIST CSF PR.IP-12 (vulnerability management) and confirm patch SLA compliance meets your defined thresholds for High-severity KEV items.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if any endpoint shows confirmed child process execution from AcroRd32.exe or Acrobat.exe (indicating successful CVE-2026-34621 exploitation), if any finance, legal, or executive endpoint accessed external PDFs within 30 days and cannot be ruled out as a victim, or if a CISA KEV remediation deadline breach is imminent — all three conditions trigger potential regulatory breach notification obligations depending on data classification of files accessible from compromised endpoints.

Recovery Notes	Before re-enabling PDF workflows, confirm every endpoint's installed Acrobat/Reader version matches the fixed version published in APSB26-43 using a PSRemoting-based version audit — do not rely on patch deployment success reports alone, as failed-silent installs are common with Adobe MSP updates. Monitor AcroRd32.exe and Acrobat.exe process trees for a minimum of 14 days post-patch using Sysmon Event ID 1 and network connection Event ID 3, specifically watching for cmd.exe, powershell.exe, wscript.exe, or rundll32.exe child processes and any outbound network connections, which would indicate a persistence mechanism planted during pre-patch exploitation. Any anomalous activity detected during this window should be treated as a confirmed pre-patch compromise and trigger full endpoint forensic acquisition.
Forensic Artifacts	Sysmon Event ID 1 (Process Creation) logs filtered on ParentImage containing 'AcroRd32.exe' or 'Acrobat.exe' — prototype pollution exploitation of CVE-2026-34621 achieving ACE would manifest here as cmd.exe, powershell.exe, wscript.exe, or mshta.exe child processes, which is not normal behavior for PDF rendering | File system artifacts under %APPDATA%\Adobe\Acrobat\DC\JavaScripts\ and %TEMP%\ for .js, .exe, .dll, or .bat files with creation timestamps coinciding with PDF open events — Acrobat's JavaScript engine is the attack surface for this prototype pollution vulnerability and payloads may stage via the plugin JavaScript directory | Memory dump of running AcroRd32.exe or Acrobat.exe processes captured via ProcDump on any endpoint with suspicious child process activity — heap analysis may reveal in-flight exploit code or shellcode injected via prototype pollution of the V8/Acrobat JS engine object prototype chain | Browser download history databases (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History SQLite; Edge: WebCacheV01.dat; Firefox: places.sqlite) queried for .pdf downloads from external domains in the 30-day pre-detection window, establishing the delivery vector timeline for CVE-2026-34621 exploitation attempts | Windows Security Event ID 4688 (Process Creation with command-line logging enabled) and Sysmon Event ID 3 (Network Connection) for any outbound connections initiated by AcroRd32.exe or Acrobat.exe — successful ACE via CVE-2026-34621 would typically be followed by a C2 callback or payload retrieval, and Acrobat has no legitimate reason to initiate outbound TCP connections during PDF rendering

Per-Action IR Details

Step 1: Containment — Identify all endpoints running Adobe Acrobat or Adobe Reader. Disable or restrict PDF opening in Acrobat/Reader via Group Policy or endpoint management until patching is confirmed. Prioritize internet-facing systems and endpoints used by finance, legal, and executive staff who routinely open external PDFs. Reference: Adobe APSB26-43.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose containment strategy based on potential damage, need for evidence preservation, and service availability; document all actions taken.

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality) — restrict AcroRd32.exe/Acrobat.exe from launching child processes via AppLocker or Software Restriction Policies, CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software) — treat unpatched Acrobat/Reader as unauthorized pending patch confirmation

Compensating: On endpoints without enterprise management: push a GPO or registry key disabling the Adobe PDF shell handler (HKCR\.pdf default value) to prevent automatic open-in-Acrobat behavior. For Sysmon-monitored hosts, deploy Sysmon Event ID 1 filtering on Image path containing 'AcroRd32.exe' or 'Acrobat.exe' with ParentImage alerts. Use PowerShell: `Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*' | Where-Object {$_.DisplayName -like '*Adobe*'} | Select DisplayName,DisplayVersion` to enumerate all affected installs across hosts via PSRemoting without an asset management tool.

Evidence: Before restricting PDF launch, capture: (1) Windows Security Event Log Event ID 4688 (Process Creation) for AcroRd32.exe and Acrobat.exe with full command-line logging enabled — these establish a baseline of normal PDF open behavior vs. any already-occurring exploit chains; (2) Sysmon Event ID 1 logs from the past 72 hours filtering on ParentImage containing 'AcroRd32.exe' or 'Acrobat.exe' to identify any child processes already spawned pre-containment; (3) file system timestamps under %APPDATA%\Adobe\Acrobat\ and %TEMP%\ for recently written .js, .exe, or .dll files that may indicate prototype pollution payload staging.

Step 2: Detection — Search endpoint detection logs for suspicious child processes spawned by AcroRd32.exe or Acrobat.exe (e.g., cmd.exe, powershell.exe, wscript.exe). In SIEM, query for T1059.007 and T1203 process creation events parented to Adobe Reader or Acrobat. Review browser download logs for PDF files delivered from external sources in the past 30 days. No confirmed IOC hashes or C2 infrastructure are available from current sources.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Use all available data sources to determine scope, entry vector, and whether exploitation has already occurred; correlate process creation, network, and file events.

Controls: NIST IR-5 (Incident Monitoring), NIST AU-12 (Audit Record Generation) — ensure process creation auditing with command-line parameters is enabled on all endpoints, NIST SI-4 (System Monitoring) — monitor for anomalous child process trees rooted at AcroRd32.exe or Acrobat.exe, CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1203 (Exploitation for Client Execution) — primary technique; prototype pollution in Acrobat JS engine leading to memory corruption and code execution, MITRE ATT&CK T1059.007 (Command and Scripting Interpreter: JavaScript) — Acrobat's embedded JavaScript engine is the attack surface for this prototype pollution vulnerability

Compensating: Without SIEM: run the following PowerShell one-liner via PSRemoting across all endpoints to extract Sysmon Event ID 1 entries where ParentImage matches Acrobat: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'AcroRd32.exe|Acrobat.exe' -and $_.Id -eq 1} | Select-Object TimeCreated,Message | Export-Csv acrobat_procs.csv`. For browser download history, parse Chrome's SQLite history DB at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\History` using `sqlite3 History 'SELECT url,last_visit_time FROM downloads WHERE target_path LIKE "%.pdf"'` to identify externally sourced PDFs opened in the 30-day window. Deploy the Florian Roth Sigma rule for 'Suspicious Acrobat Reader Child Process' (available in the SigmaHQ repository) converted to Windows Event Log format for manual grep if no SIEM is available.

Evidence: Capture before pivoting to eradication: (1) Sysmon Event ID 3 (Network Connection) logs for outbound connections initiated by AcroRd32.exe or Acrobat.exe — prototype pollution exploitation leading to ACE would typically be followed by a callback or payload fetch; (2) Windows Security Event ID 4688 with command-line logging for any cmd.exe, powershell.exe, wscript.exe, or mshta.exe where ParentProcessName contains 'AcroRd32' or 'Acrobat'; (3) browser download logs (Chrome History SQLite, Edge WebCacheV01.dat, Firefox places.sqlite) for .pdf files sourced from external domains in the past 30 days — these are the likely delivery vector for CVE-2026-34621 exploitation; (4) %TEMP% and %APPDATA%\Adobe\Acrobat\DC\JavaScripts\ directories for any .js files written or modified within the detection window, as prototype pollution payloads frequently stage via Acrobat's JavaScript plugin directory.

Step 3: Eradication — Apply the patch detailed in Adobe Security Bulletin APSB26-43 (https://helpx.adobe.com/security/products/acrobat/apsb26-43.html). Verify the installed version against the patched version matrix in that bulletin. If patching is not immediately possible, consider deploying Adobe Acrobat's Protected View mode (sandboxed rendering) as a temporary mitigation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: After containment, identify and eliminate all components of the incident including the vulnerability enabling initial access; confirm eradication before restoration.

Controls: NIST SI-2 (Flaw Remediation) — identify, report, and correct the Adobe Acrobat/Reader flaw per vendor advisory APSB26-43; test patch for effectiveness before broad deployment, NIST CM-7 (Least Functionality) — enforce Protected View (sandboxed rendering) as a compensating control where patch cannot be immediately applied, CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.4 (Perform Automated Application Patch Management) — CVE-2026-34621 is a KEV item with CISA remediation deadline of April 27, 2026; patch SLA is non-negotiable

Compensating: If SCCM/Intune is unavailable, use Adobe's provided MSI/MSP installer from APSB26-43 with a silent push via PSRemoting: `Invoke-Command -ComputerName (Get-Content hosts.txt) -ScriptBlock {Start-Process msiexec -ArgumentList '/update C:\Patches\AcrobatPatch.msp /qn /norestart' -Wait}`. To enforce Protected View immediately as a compensating control without patching, push the registry key `HKCU\Software\Adobe\Acrobat Reader\DC\TrustManager` with `bEnhancedSecurityStandalone=1` and `bProtectedMode=1` via GPO or a PSRemoting loop. Verify Protected View is active post-push by checking the same keys: `Get-ItemProperty 'HKCU:\Software\Adobe\Acrobat Reader\DC\TrustManager'`.

Evidence: Before patching, preserve: (1) a full disk image or at minimum a forensic copy of %APPDATA%\Adobe\, %TEMP%\ (filtered for Adobe-related artifacts), and the Acrobat/Reader installation directory (typically C:\Program Files (x86)\Adobe\Acrobat Reader DC\) from any endpoint showing suspicious child process activity — these preserve potential exploit payload artifacts before patch overwrites them; (2) memory dump of any running AcroRd32.exe or Acrobat.exe processes on suspected-compromised hosts using ProcDump (`procdump -ma AcroRd32.exe acrobat_memdump.dmp`) — prototype pollution exploits manipulate the JavaScript engine heap and a memory dump may capture in-flight shellcode or payload; (3) a registry export of `HKCU\Software\Adobe` and `HKLM\SOFTWARE\Adobe` for pre-patch version confirmation and post-patch change validation.

Step 4: Recovery — After patching, validate the installed version on all endpoints against the fixed version listed in APSB26-43. Re-enable PDF workflows. Monitor AcroRd32.exe and Acrobat.exe process trees for 14 days post-patch for any anomalous child process activity that could indicate a pre-patch compromise still persisting.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation, confirm systems are functioning normally, and implement additional monitoring to detect recurrence or persistence mechanisms installed prior to patching.

Controls: NIST IR-4 (Incident Handling) — recovery actions must be consistent with the incident response plan; verify eradication before restoring PDF workflows, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of patched Acrobat/Reader installation against Adobe-published checksums from APSB26-43, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — maintain heightened review cadence of AcroRd32.exe/Acrobat.exe process tree logs for 14 days post-recovery, CIS 7.2 (Establish and Maintain a Remediation Process) — confirm patched version meets APSB26-43 fixed-version matrix before re-enabling PDF workflows

Compensating: Without EDR for 14-day post-patch monitoring: configure a Sysmon rule targeting Event ID 1 with ParentImage filtering on AcroRd32.exe or Acrobat.exe and pipe output to a daily scheduled task that emails a CSV digest: `schtasks /create /tn 'AcrobatChildProcAudit' /tr 'powershell -File C:\Scripts\acrobat_monitor.ps1' /sc daily /st 06:00`. Use osquery with a persistent scheduled query: `SELECT name,path,cmdline,parent FROM processes WHERE parent IN (SELECT pid FROM processes WHERE name IN ('AcroRd32.exe','Acrobat.exe'))` run every 5 minutes and logged to a central file share for manual review. For version validation without SCCM, run: `Get-WmiObject -Class Win32_Product -Filter "Name LIKE '%Adobe%'" | Select Name,Version` across all hosts via PSRemoting and compare output to APSB26-43 fixed-version table.

Evidence: During the 14-day monitoring window, preserve on an ongoing basis: (1) Sysmon Event ID 1 logs for all child processes of AcroRd32.exe and Acrobat.exe — a persistence mechanism (scheduled task, registry run key, DLL planted in Acrobat's plugin directory) installed before patching would continue to execute post-patch and would appear here; (2) Windows Security Event ID 4698/4702 (Scheduled Task Created/Modified) and Event ID 4657 (Registry Value Modified) around the Acrobat plugin and startup key paths, which would indicate an attacker-planted persistence mechanism surviving the patch; (3) network flow logs or Sysmon Event ID 3 for any outbound connections from AcroRd32.exe or Acrobat.exe post-patch — patched Acrobat should not initiate outbound connections during normal PDF rendering.

Step 5: Post-Incident — Review PDF handling policies: assess whether all staff require full Acrobat/Reader or whether a lighter, less attack-surface-heavy viewer is appropriate for general use. Evaluate whether application allowlisting or sandboxing is enforced for document viewer applications. Map this vulnerability to NIST CSF PR.IP-12 (vulnerability management) and confirm patch SLA compliance meets your defined thresholds for High-severity KEV items.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct lessons-learned meeting, update detection rules and policies based on incident findings, and share intelligence to improve organizational and community defenses.

Controls: NIST IR-4 (Incident Handling) — update incident handling capability based on lessons learned from CVE-2026-34621 response, NIST IR-8 (Incident Response Plan) — revise IR plan to include Adobe Acrobat/Reader as a named high-risk application category requiring expedited patch SLA for future KEV disclosures, NIST SI-2 (Flaw Remediation) — formalize patch SLA policy that treats CISA KEV items as P1 regardless of internal CVSS scoring; CVE-2026-34621's April 27, 2026 deadline must be codified as a compliance threshold, NIST RA-5 (Vulnerability Monitoring and Scanning) — add Adobe Acrobat/Reader version compliance to recurring vulnerability scan policy, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update vulnerability management process to explicitly include CISA KEV catalog as a mandatory input source, CIS 2.2 (Ensure Authorized Software is Currently Supported) — assess whether Adobe Acrobat/Reader versions deployed are currently supported; evaluate lighter PDF viewers (e.g., SumatraPDF) for non-power-user populations to reduce attack surface

Compensating: For application allowlisting without commercial tooling: deploy Windows Defender Application Control (WDAC) policy in audit mode first, then enforce mode, restricting document viewer applications to an approved list. Use AppLocker Path Rules to block execution of AcroRd32.exe or Acrobat.exe for user populations that do not require it (e.g., allow only for finance/legal OUs via scoped GPO). For sandboxing without a commercial sandbox, validate that Adobe Protected View (configured in Step 3) is enforced persistently via GPO and confirmed active via registry audit script run weekly. Document this architecture in a one-page PDF Handling Policy referencing APSB26-43 as the forcing function.

Evidence: For the post-incident report, collect and preserve: (1) the full timeline of APSB26-43 publication date vs. organizational patch completion date — this gap is the metrics input for SLA compliance reporting under NIST SI-2 (Flaw Remediation); (2) a final endpoint inventory report showing patched Acrobat/Reader version vs. APSB26-43 fixed-version matrix for all assets, exported from patch management or PSRemoting scan, to serve as audit evidence; (3) any Sysmon or SIEM detections of AcroRd32.exe or Acrobat.exe spawning child processes during the incident window — these become the basis for updated detection rules and Sigma content; (4) documentation of any endpoints where Protected View could not be enforced or where patching was delayed, with business justification, to support risk acceptance and exception management processes.

Detection Guidance

Query endpoint telemetry for process creation events where the parent process is AcroRd32.exe or Acrobat.exe and the child process is a shell, scripting host, or network utility (cmd.exe, powershell.exe, wscript.exe, mshta.exe, certutil.exe). In Windows Event Logs, monitor Event ID 4688 (process creation) with the above parent-child patterns. In EDR platforms, search for T1059.007 (JavaScript/scripting engine abuse) and T1203 (client-side exploitation) tagged against Adobe processes. No confirmed IOCs (hashes, IPs, domains) are available from current sources, behavioral detection is the primary method at this time. Flag any PDF files opened from email or web sources on unpatched endpoints for retroactive review.

Framework Mappings

MITRE-ATTACK

- **T1059.007** — JavaScript
- **T1203** — Exploitation for Client Execution

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring
- **AC-6** — Least Privilege

ISO-27001-2022

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

NIST-CSF-2

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

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059.007	JavaScript	Execution
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Adobe Security Bulletin - Adobe Help Center	https://helpx.adobe.com/security/products/acrobat/apsb26-43.html	T3
CVE-2026-34621 | Tenable®	https://www.tenable.com/cve/CVE-2026-34621	T3
CVE-2026-34621 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
Adobe Patches Actively Exploited Acrobat Reader Flaw CVE-2026 ...	https://www.cypro.se/2026/04/12/adobe-patches-actively-exploited-ac...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34621	T1

Source	URL	Tier
Adobe Security Advisory	https://helpx.adobe.com/security/products.html	T1

Generated 2026-04-13 16:28 UTC by TJS Security Command Center