INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 18:52 UTC

CISA KEV Catalog Updated: One New Actively Exploited Vulnerability Added (2026-05-22)

GOVERNANCE | HIGH

SCC Item ID	SCC-GOV-2026-0055
Type	Governance
Severity	HIGH
Affected Products	Unspecified, specific CVE and affected product not extractable from source data
Published	2026-06-11
Discovery Source	Gemini

Executive Summary

CISA updated its Known Exploited Vulnerabilities Catalog on 2026-05-22, adding one vulnerability confirmed as actively exploited in the wild. The specific CVE identifier and affected product were not available in the source data; direct review of the CISA advisory is required to assess organizational exposure. Federal Civilian Executive Branch agencies face a mandatory remediation deadline under BOD 22-01, and all organizations should treat KEV additions as high-priority signals regardless of federal mandate.

Technical Analysis

CISA added one entry to the KEV Catalog on 2026-05-22 under the authority of Binding Operational Directive 22-01. The specific CVE ID, affected vendor, affected product, and exploitation mechanism were not extractable from the available source data. No CVSS base score, EPSS score, CWE classification, or MITRE ATT&CK technique mappings are available from this data set. The CISA advisory at https://www.cisa.gov/news-events/alerts/2026/05/22/cisa-adds-one-known-exploited-vulnerability-catalog should be consulted directly to obtain the CVE identifier, affected product version, exploitation vector, and FCEB remediation due date. Until that review is complete, treatment as a high-severity item is consistent with KEV catalog policy and the qualitative rating assigned by the upstream pipeline.

Action Checklist

1. Step 1: Containment. Retrieve the specific CVE ID and affected product from the CISA advisory at https://www.cisa.gov/news-events/alerts/2026/05/22/cisa-adds-one-known-exploited-vulnerability-catalog

before taking further action. Do not assume scope without the CVE. If the affected product is identified and is internet-facing in your environment, isolate or restrict access to that service immediately in coordination with your incident response and business continuity teams, pending patch verification.

2. Step 2: Detection. Cross-reference the retrieved CVE ID against your asset inventory (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory) to identify affected systems. Query your SIEM for the affected product name and version once known. Review audit logs per NIST AU-6 (Audit Record Review, Analysis, and Reporting) for anomalous activity on any identified assets dating back at least 30 days.

3. Step 3: Eradication. Apply the vendor-supplied patch identified in the CISA advisory. FCEB agencies must remediate within the CISA-specified due date under BOD 22-01. All other organizations should follow their documented remediation process per CIS 7.2 (Establish and Maintain a Remediation Process) and NIST SI-2 (Flaw Remediation), prioritizing this item as a confirmed in-the-wild exploitation.

4. Step 4: Recovery. After patching, validate system integrity using file integrity monitoring aligned with NIST SI-7 (Software, Firmware, and Information Integrity) and D3FEND countermeasure D3-SFA (System File Analysis). Re-enable any services restricted during containment only after patch confirmation. Continue monitoring per NIST SI-4 (System Monitoring) for post-exploitation indicators on previously exposed assets.

5. Step 5: Post-Incident. Document the response timeline and any gaps in asset visibility that delayed detection of exposure. Evaluate whether automated patch management (CIS 7.3: Perform Automated Operating System Patch Management; CIS 7.4: Perform Automated Application Patch Management) would have reduced time-to-remediation. Review KEV monitoring processes to ensure future catalog additions trigger immediate triage within your vulnerability management workflow (CIS 7.1: Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if log review confirms successful exploitation of the affected product during the 30-day lookback window, if the affected system processes PII, PHI, or financial data triggering breach notification requirements, or if the organization is an FCEB agency and cannot meet the BOD 22-01 remediation deadline.
Recovery Notes	After patching, do not treat the affected system as clean until the full 30-day pre-patch log window has been reviewed for indicators of successful exploitation, as KEV-listed vulnerabilities are confirmed in-the-wild and dwell time may predate organizational awareness. Re-enable internet-facing services only after patch version is confirmed and file integrity validation passes. Maintain heightened monitoring on previously exposed assets for a minimum of 30 days post-recovery, focusing on anomalous child process spawning, new persistence mechanisms, and lateral movement indicators consistent with post-exploitation activity.

Forensic Artifacts	Web server access logs (IIS: %SystemDrive%\inetpub\logs\LogFiles\; Apache/nginx: /var/log/apache2/ or /var/log/nginx/) covering the 30-day pre-patch window — filter for HTTP status codes 200/500 against the affected service endpoint to identify successful versus failed exploitation attempts once the CVE attack vector is retrieved from the CISA advisory. | Volatile network state captured pre-isolation: `netstat -ano` (Windows) or `ss -tunap` (Linux) output recording all established and listening connections on the affected service port, which may reveal active attacker sessions or C2 beaconing initiated post-exploitation. | Windows Security Event Log entries: Event ID 4688 (Process Creation with command-line logging enabled via Sysmon or audit policy) filtering for unusual child processes spawned by the affected service executable, and Event ID 4624/4625 (Logon Success/Failure) on the affected host for the exposure window. | Scheduled task and service creation logs: Windows Event ID 4698 (Scheduled Task Created) and 7045 (New Service Installed) from the System event log, and Linux `/etc/cron*`, `/var/spool/cron/`, and `/etc/systemd/system/` for entries created during the exposure window — common persistence mechanisms deployed after initial access via a KEV-class vulnerability. | Pre-patch binary hash record: SHA-256 hash of the affected application's primary executable and libraries captured before patching, retained as forensic evidence of the vulnerable version state and to support any future chain-of-custody requirement if exploitation is confirmed.

Per-Action IR Details

Step 1: Containment — Retrieve the specific CVE ID and affected product from the CISA advisory at https://www.cisa.gov/news-events/alerts/2026/05/22/cisa-adds-one-known-exploited-vulnerability-catalog before taking further action. Do not assume scope without the CVE. If the affected product is identified and is internet-facing in your environment, isolate or restrict access to that service immediately pending patch verification.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without SIEM or enterprise NAC, use host-based firewall rules to block inbound connections to the affected service port immediately: on Windows, run `netsh advfirewall firewall add rule name='KEV-BLOCK' dir=in action=block protocol=tcp localport=`; on Linux, `iptables -I INPUT -p tcp --dport -j DROP`. Maintain a change log with timestamp and operator name. If the product is a web service, place it behind a reverse proxy (nginx) with a temporary 503 maintenance page to deny external access while preserving the host for forensic capture.

Evidence: BEFORE isolating any internet-facing asset: capture active TCP connections with `netstat -ano` (Windows) or `ss -tunap` (Linux) and record all established sessions to the affected service port. Capture running process list (`tasklist /v` or `ps auxf`). Export current web server access logs (IIS: `%SystemDrive%\inetpub\logs\LogFiles\`, Apache/nginx: `/var/log/`) covering at least the past 30 days — these logs may contain pre-patch exploitation attempts referencing the specific CVE's attack vector URI or payload pattern once the CVE is retrieved.

Step 2: Detection — Cross-reference the retrieved CVE ID against your asset inventory (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory) to identify affected systems. Query your SIEM for the affected product name and version once known. Review audit logs per NIST AU-6 (Audit Record Review, Analysis, and Reporting) for anomalous activity on any identified assets dating back at least 30 days.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use osquery to enumerate affected product installations across endpoints: `SELECT name, version, install_location FROM programs WHERE name LIKE '%%';` (Windows) or query the `deb_packages` / `rpm_packages` tables on Linux hosts. Correlate against a flat asset CSV. For log review without SIEM, use PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.TimeCreated -gt (Get-Date).AddDays(-30)}` filtered on Event ID 4688 (Process Creation) for child processes spawned by the affected service. On Linux, use `grep -E '' /var/log/auth.log /var/log/syslog` once the CVE mechanism is known.

Evidence: This step performs read-only analysis and does not alter live state, so order-of-volatility risk is low; however, if an affected host is found to be actively compromised during triage, immediately acquire RAM (WinPmem or LiME) and volatile network state before any remediation action. Key artifacts to pull during detection: web server access logs for the 30-day lookback window (filter on HTTP 200/500 response codes to the affected service endpoint), authentication logs for accounts associated with the affected service (Windows Security Event ID 4624/4625), and installed software version data from the asset inventory to confirm version-level exposure.

Step 3: Eradication — Apply the vendor-supplied patch identified in the CISA advisory. FCEB agencies must remediate within the CISA-specified due date under BOD 22-01. All other organizations should follow their documented remediation process per CIS 7.2 (Establish and Maintain a Remediation Process) and NIST SI-2 (Flaw Remediation), prioritizing this item as a confirmed in-the-wild exploitation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without automated patch management, create a scripted patch deployment workflow: download the vendor patch to a staging server, verify SHA-256 hash against the vendor advisory, then push via PSExec or Ansible ad-hoc command (`ansible affected_hosts -m win_updates` / `-m yum`/`apt`) to all identified affected systems. Maintain a patch log (hostname, patch KB/version, timestamp, operator) as audit evidence for BOD 22-01 compliance documentation. For FCEB agencies without centralized patching, prioritize internet-facing instances first and document the remediation order with timestamps.

Evidence: BEFORE applying the patch, and only if the host has not already been forensically preserved in Step 1: acquire full RAM image (WinPmem for Windows, LiME kernel module for Linux), capture `netstat -ano` / `ss -tunap` output, export the affected service's process memory if feasible, and preserve all web server and application logs in their pre-patch state. Patching modifies or replaces vulnerable binaries — once applied, the vulnerable code state that could confirm exploit execution is overwritten. Record the pre-patch software version string as evidence of exposure scope.

Step 4: Recovery — After patching, validate system integrity using file integrity monitoring aligned with NIST SI-7 (Software, Firmware, and Information Integrity) and D3FEND countermeasure D3-SFA (System File Analysis). Re-enable any services restricted during containment only after patch confirmation. Continue monitoring per NIST SI-4 (System Monitoring) for post-exploitation indicators on previously exposed assets.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, And Information Integrity), NIST SI-4 (System Monitoring), MITRE D3FEND D3-SFA (System File Analysis)

Compensating: Without enterprise FIM, use AIDE (Linux) or Windows built-in `sfc /scannow` plus PowerShell `Get-FileHash` to baseline and verify critical system files and the patched application binaries post-remediation. On Linux: `aide --check` against a pre-compromise baseline, or generate a new baseline post-patch with `aide --init`. Deploy a Sigma rule targeting process creation events from the previously affected service to detect post-patch anomalous child process spawning (e.g., cmd.exe, powershell.exe, curl as children of the affected service process) using Sysmon Event ID 1.

Evidence: After re-enabling services, monitor web server access logs and authentication logs for recurrence of the same attack-vector URI patterns or payload signatures identified during the detection phase. Because active

exploitation of a KEV-listed vulnerability may indicate a dwell-time compromise predating discovery, watch for persistence indicators specific to the affected platform: scheduled tasks (Windows Event ID 4698), new service installations (Event ID 7045), and cron job modifications (`/etc/cron*`, `/var/spool/cron/`) created during the exposure window.

Step 5: Post-Incident — Document the response timeline and any gaps in asset visibility that delayed detection of exposure. Evaluate whether automated patch management (CIS 7.3: Perform Automated Operating System Patch Management; CIS 7.4: Perform Automated Application Patch Management) would have reduced time-to-remediation. Review KEV monitoring processes to ensure future catalog additions trigger immediate triage within your vulnerability management workflow (CIS 7.1: Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Conduct a structured lessons-learned meeting within 5 business days using a written agenda covering: (1) time elapsed from KEV publication to internal triage, (2) asset inventory completeness for the affected product, (3) patch availability-to-deployment gap. Document findings in a simple after-action report template. For FCEB agencies, retain this documentation as BOD 22-01 compliance evidence. Configure a free CISA KEV RSS feed alert (`https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) polled via a cron job or low-code automation (n8n, Huginn) to trigger a triage ticket on every new catalog entry.

Evidence: Preserve all response documentation as post-incident artifacts: the response timeline log with operator actions and timestamps, the pre-patch asset inventory query results showing affected system count, patch deployment confirmation records (version strings before and after), and any SIEM/log queries run during detection. If exploitation was confirmed during the lookback review, retain the relevant log excerpts as evidence and assess whether regulatory breach notification obligations apply based on data classification of the affected system.

Detection Guidance

Specific detection queries and IOC patterns cannot be provided until the CVE ID and affected product are retrieved from the CISA advisory. Once identified: search SIEM logs for the affected product and version across your asset inventory; review NIST AU-2 (Event Logging) sources for the affected system category; and check for exploitation-pattern indicators specified in the vendor advisory. Apply NIST SI-4 (System Monitoring) continuous monitoring to any confirmed affected assets. No IOCs are available from the current source data. CISA's KEV catalog entry and the linked vendor advisory will contain authoritative exploitation indicators. No mapped detection rule can be provided from this data set without fabricating specifics.

Framework Mappings

ISO-27001-2022

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

SOC2-TSC

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

NIST-800-53R5

- **SI-4** — System Monitoring

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

Sources

Source	URL	Tier
gemini	https://www.cisa.gov/news-events/alerts-advisories/cybersecurity-al...	T1
Known Exploited Vulnerabilities Catalog - CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Known Exploited Vulnerabilities Catalog - CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog-print	T1
CISA Adds One Known Exploited Vulnerability to Catalog | CISA	https://www.cisa.gov/news-events/alerts/2026/05/22/cisa-adds-one-kn...	T1
What is the Known Exploited Vulnerabilities Catalog (KEV)?	https://www.armosec.io/glossary/known-exploited-vulnerabilities-cat...	T3

Generated 2026-06-12 18:52 UTC by TJS Security Command Center