INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-28 06:46 UTC

Before the Ransom Note: Reconstructing Akira's Pre-Encryption Kill Chain from Log Evidence

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0377
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Organizations targeted by Akira ransomware; specific perimeter and endpoint systems not enumerated in available source text
Published	2026-05-27T17:14:03
Discovery Source	Rss

Executive Summary

Akira ransomware operators follow a consistent pre-encryption kill chain, exploiting weak authentication at the perimeter, escalating privileges, and moving laterally before deploying ransomware, and new forensic analysis from SANS ISC shows these stages leave recoverable log evidence defenders can act on. Organizations running internet-facing VPN or remote access infrastructure with single-factor authentication are the primary target profile. The business risk is operational shutdown, data theft before encryption, and extortion; early detection using the documented log artifacts can disrupt the attack before encryption occurs.

Technical Analysis

This SANS ISC forensic walkthrough reconstructs Akira ransomware's pre-encryption kill chain from perimeter and endpoint log evidence. No CVE is associated with this campaign. The kill chain maps to three under-documented phases: initial access via valid account abuse or authentication bypass (CWE-287, CWE-308; MITRE T1078, T1078.002, T1133), privilege escalation using living-off-the-land techniques (T1548, T1059, T1543.003), and lateral movement via SMB/Windows Admin Shares and WMI (T1021, T1021.002, T1047). Supporting reconnaissance includes domain account enumeration (T1087.002, T1069.002), process discovery (T1057), and file system enumeration (T1083). Akira operators clear Windows event logs pre-encryption (T1070.001), a high-fidelity indicator of imminent ransomware deployment. CWE-532 is relevant: log artifacts may inadvertently expose credential material useful during forensic reconstruction. The campaign does not exploit a specific patched CVE; the attack surface is authentication architecture and detection gaps, not unpatched software. The primary source is a SANS ISC forensic walkthrough, a Tier 1 authority for incident

analysis methodology.

Action Checklist

1. Containment, Audit all internet-facing remote access services (VPN concentrators, RDP gateways, external-facing RMM tools) and verify MFA is enforced on every authentication path per CIS 6.3 and CIS 6.4. Restrict or segment any service running single-factor authentication until MFA is confirmed active. Reference NIST AC-17 for remote access configuration requirements.
2. Detection, Hunt for Akira pre-encryption indicators across endpoint and perimeter logs: (1) Windows Security Event ID 4625/4624 clusters showing failed then successful logins from external IPs, especially against VPN or RDP; (2) Event ID 1102 or 104 (Security/System log clear), Akira clears logs pre-encryption per T1070.001, treat this as a high-priority alert; (3) WMI activity (Event ID 4688, process name wmiprvse.exe spawning cmd.exe or powershell.exe) per T1047; (4) Lateral SMB connections to ADMIN$ or C$ shares (Event ID 5140) from unexpected source hosts per T1021.002; (5) LDAP/net.exe queries enumerating domain groups or accounts (T1087.002, T1069.002). Cross-reference against NIST AU-6 review requirements.
3. Eradication, This campaign does not exploit a patchable CVE. Eradication requires closing the authentication and detection gaps Akira exploits: (1) Enforce phishing-resistant MFA on all external-facing services (CIS 6.3, CIS 6.4, NIST AC-7); (2) Rotate credentials for any account showing anomalous login activity per NIST AC-2 account management requirements; (3) Disable or restrict WMI remote execution where not operationally required (reduces T1047 exposure); (4) Audit and harden local and domain admin account usage per NIST AC-6 and CIS 5.4, restrict admin privileges to dedicated admin accounts only.
4. Recovery, After credential rotation and MFA enforcement: (1) Validate Windows event log integrity across all affected endpoints, confirm logs are present and unmodified (NIST AU-9); (2) Verify no scheduled tasks or services were created by the attacker (T1543.003, review Task Scheduler and Services registry keys); (3) Confirm no persistence mechanisms remain via startup config analysis (NIST AC-2, AC-6); (4) Re-enable full audit logging per NIST AU-2 and AU-12 and confirm log forwarding to SIEM is active per CIS 8.2; (5) Monitor for resumed lateral movement attempts for 72 hours post-remediation.
5. Post-Incident, Akira's success in documented intrusions traces to two systemic gaps: single-factor authentication on perimeter systems and insufficient alerting on log-clearing events. Formalize: (1) A detection rule for Event ID 1102/104 firing as a P1 alert (addresses T1070.001 and NIST SI-4 monitoring gaps); (2) Quarterly MFA coverage audit across all external-facing services (CIS 6.3, CIS 6.4); (3) Log retention policy review against NIST AU-11, ensure retention supports the forensic lookback window Akira's dwell time requires; (4) Tabletop exercise simulating Akira's kill chain phases to validate playbook coverage for pre-encryption disruption.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if Event ID 1102 or 104 is confirmed on any endpoint (indicating active log clearing per T1070.001), if any domain admin account shows lateral movement artifacts, or if data exfiltration to external infrastructure is detected — all three conditions suggest Akira's pre-encryption phase is active and ransomware deployment is imminent, triggering breach notification assessment under applicable regulations (HIPAA, state breach laws) if PII or PHI is in scope.
Recovery Notes	After MFA enforcement and credential rotation, verify that no WMI subscriptions, scheduled tasks, or rogue services created during Akira's dwell period survive on any endpoint that experienced lateral movement (Event ID 5140 ADMIN$/C$ access) — these are Akira's known persistence vectors and their presence invalidates recovery. Restore and validate Windows event log continuity on all affected hosts before resuming normal operations, as gaps in log timestamps indicate Akira's T1070.001 activity and suggest additional forensic investigation is required. Maintain elevated monitoring of domain controller authentication logs (Event ID 4624 Type 3) and SMB share access (Event ID 5140) for a minimum of 72 hours post-remediation, as Akira operators have been observed re-entering environments through secondary compromised accounts not identified in initial triage.
Forensic Artifacts	Windows Security Event Log (evtx) — specifically Event ID 4624/4625 clusters from external source IPs against VPN-adjacent or RDP-exposed hosts, which reconstruct Akira's credential-based initial access phase and identify the compromised account(s) | Windows Security Event Log Event ID 1102 and System Log Event ID 104 — presence of these events is a direct forensic indicator of Akira's T1070.001 log-clearing behavior in the pre-encryption phase; their timestamps anchor the kill chain timeline | Sysmon Event ID 1 (Process Creation) logs capturing wmiprvse.exe spawning cmd.exe or powershell.exe — the specific process chain Akira uses for T1047 WMI-based lateral execution, recoverable from Sysmon Operational log at 'Microsoft-Windows-Sysmon/Operational' | WMI repository artifacts at 'C:\Windows\System32\wbem\Repository\' and output of 'Get-WMIObject -Namespace root\subscription' queries — Akira-affiliated actors use WMI event subscriptions (T1546.003) for persistence that survives reboots and is not visible in standard task or service enumeration | Windows Security Event ID 5140 (Network Share Object Access) entries on domain controllers and file servers showing ADMIN$ and C$ access from non-administrative source hosts — these map Akira's lateral movement path (T1021.002) and identify the full scope of compromised endpoints beyond the initial access point

Per-Action IR Details

Containment — Audit all internet-facing remote access services (VPN concentrators, RDP gateways, external-facing RMM tools) and verify MFA is enforced on every authentication path per CIS 6.3 and CIS 6.4. Temporarily restrict or segment any service running single-factor authentication until MFA is confirmed active. Reference NIST AC-17 for remote access configuration requirements.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For teams without an enterprise MFA solution: use Windows Server NPS with RADIUS to gate VPN authentication and enforce certificate-based or OTP second factor at no cost. For RDP gateways, enable Windows RD Gateway with Network Level Authentication (NLA) and restrict RDP exposure via Windows Firewall rules — run 'netsh advfirewall firewall add rule name=RDP-Restrict protocol=TCP dir=in localport=3389 remoteip= action=allow' to limit source IPs. Enumerate all listening services with 'netstat -ano | findstr LISTENING' and cross-reference against known-good service list to identify unexpected RMM listeners.

Evidence: Before restricting services, capture: (1) VPN/RDP authentication logs showing the source IPs and usernames of all successful and failed logins from the past 30 days — Akira's initial access leverages credential stuffing or brute force against single-factor VPN endpoints, so the originating external IP cluster is a key IOC; (2) netflow or firewall session logs for the identified external IPs to determine dwell time prior to MFA enforcement; (3) active session list from the VPN concentrator or RD Gateway at time of isolation to identify any sessions that may already be actor-controlled.

Detection — Hunt for Akira pre-encryption indicators across endpoint and perimeter logs: (1) Windows Security Event ID 4625/4624 clusters showing failed then successful logins from external IPs, especially against VPN or RDP; (2) Event ID 1102 or 104 (Security/System log clear) — Akira clears logs pre-encryption per T1070.001, treat this as a high-priority alert; (3) WMI activity (Event ID 4688, process name wmiprvse.exe spawning cmd.exe or powershell.exe) per T1047; (4) Lateral SMB connections to ADMIN$ or C$ shares (Event ID 5140) from unexpected source hosts per T1021.002; (5) LDAP/net.exe queries enumerating domain groups or accounts (T1087.002, T1069.002). Cross-reference against NIST AU-6 review requirements.

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-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without SIEM: (1) Run the following PowerShell against collected Security logs to surface credential-stuffing patterns: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Group-Object {$_.Properties[19].Value} | Sort-Object Count -Descending | Select-Object -First 20' — this groups failures by source IP; (2) Deploy Sysmon with SwiftOnSecurity's config (https://github.com/SwiftOnSecurity/sysmon-config) — Sysmon Event ID 1 will capture wmiprvse.exe spawning cmd.exe or powershell.exe even without EDR; (3) Use the Sigma rule 'win_wmi_spawning_windows_shell.yml' (from the SigmaHQ repository) converted to Windows Event Log XML query format to detect T1047 process chains; (4) For SMB lateral movement, run 'Get-WinEvent -LogName Security -FilterXPath "*[System[EventID=5140]]" | Where-Object {$_.Message -like "*ADMIN$*" -or $_.Message -like "*C$*"}' on domain controllers and file servers.

Evidence: Preserve before any log rotation or clearing: (1) Full Windows Security Event Log export (evtx format) from all domain controllers, VPN-adjacent hosts, and suspected initial access targets — Event ID 4624 Type 3 (network logon) from external IPs is Akira's post-VPN-auth movement signature; (2) System Event Log (Event ID 104) and Security Event Log (Event ID 1102) entries — presence of these events on endpoints IS the forensic artifact confirming Akira's T1070.001 log-clearing behavior; (3) Sysmon Operational log (if deployed) capturing process creation chains rooted at wmiprvse.exe; (4) SMB session logs from domain controllers and file servers capturing ADMIN$ and C$ share access with source hostnames; (5) DNS query logs or domain controller netlogon.log entries showing the sequence of lateral movement targets Akira enumerated.

Eradication — This campaign does not exploit a patchable CVE. Eradication requires closing the authentication and detection gaps Akira exploits: (1) Enforce phishing-resistant MFA on all external-facing services (CIS 6.3, CIS 6.4, NIST AC-7); (2) Rotate credentials for any account showing anomalous login activity per D3-CRO; (3) Disable or restrict WMI remote execution where not operationally required (reduces T1047 exposure); (4) Audit and harden local and domain admin account usage per NIST AC-6 and CIS 5.4 — restrict admin privileges to dedicated admin accounts only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-7 (Unsuccessful Logon Attempts), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Credential rotation at scale without enterprise tooling: use 'Invoke-ADAccountAudit' via the free AD module to list all accounts with last logon timestamps matching the Akira dwell window, then force password reset via 'Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText -Force)' for each flagged

account. Restrict WMI remote access via GPO: Computer Configuration > Windows Settings > Security Settings > Windows Firewall — block inbound TCP 135 (RPC/WMI) from all hosts except known management IPs. Identify accounts with admin rights beyond dedicated admin accounts using 'Get-ADGroupMember -Identity "Domain Admins" -Recursive | Select-Object name, SamAccountName' and remediate over-provisioning immediately.

Evidence: Before rotating credentials or disabling WMI, capture: (1) Active Directory lastLogon and lastLogonTimestamp attributes for all accounts flagged in the 4624/4625 analysis — this establishes which accounts Akira likely compromised and used for lateral movement; (2) WMI subscription persistence artifacts: query 'Get-WMIObject -Namespace root\subscription -Class __EventFilter', '__EventConsumer', and '__FilterToConsumerBinding' — Akira and affiliated actors have used WMI subscriptions for persistence (T1546.003) which must be documented before eradication; (3) Local Administrators group membership on all endpoints touched during lateral movement, captured via 'net localgroup administrators' or osquery 'SELECT * FROM users JOIN groups ON groups.gid = users.gid WHERE groups.groupname = "administrators"'.

Recovery — After credential rotation and MFA enforcement: (1) Validate Windows event log integrity across all affected endpoints — confirm logs are present and unmodified (NIST AU-9); (2) Verify no scheduled tasks or services were created by the attacker (T1543.003 — review Task Scheduler and Services registry keys); (3) Confirm no persistence mechanisms remain via startup config analysis (D3-SICA); (4) Re-enable full audit logging per NIST AU-2 and AU-12 and confirm log forwarding to SIEM is active per CIS 8.2; (5) Monitor for resumed lateral movement attempts for 72 hours post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-9 (Protection of Audit Information), NIST AU-12 (Audit Record Generation), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 8.2 (Collect Audit Logs)

Compensating: Log integrity validation without a SIEM: use 'wevtutil gl Security' to confirm the current log size and last write time matches expected values — a gap in timestamps or a log smaller than baseline is a T1070.001 indicator. Enumerate all scheduled tasks created during the suspected dwell window using 'schtasks /query /fo LIST /v | findstr /i "task name\|next run\|last run\|status\|run as"' and cross-reference creation timestamps against the Akira intrusion timeline. For service persistence, query 'Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services* | Where-Object {$_.ImagePath -like "*cmd*" -or $_.ImagePath -like "*powershell*" -or $_.ImagePath -like "*wscript*"}' — Akira has used service-based persistence with LOLBin image paths. Re-enable and verify Sysmon log forwarding to a central syslog server (even a free Graylog CE instance) before declaring recovery complete.

Evidence: Before declaring recovery: (1) Hash all restored or verified-clean event log files (evtx) using 'Get-FileHash -Algorithm SHA256' and store externally — this creates a post-incident baseline for future comparison and supports any regulatory evidence requirements; (2) Export the full scheduled task XML definitions from 'C:\Windows\System32\Tasks\' on all affected hosts and diff against a known-good baseline or CIS benchmark task list; (3) Export registry run keys from 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run', and WMI subscription namespaces to confirm no Akira persistence survived eradication; (4) Capture a memory image (via WinPmem, free) from any host where log-clearing events were confirmed — memory may contain injected code or credential material that disk artifacts do not.

Post-Incident — Akira's success in documented intrusions traces to two systemic gaps: single-factor authentication on perimeter systems and insufficient alerting on log-clearing events. Formalize: (1) A detection rule for Event ID 1102/104 firing as a P1 alert (addresses T1070.001 and NIST SI-4 monitoring gaps); (2) Quarterly MFA coverage audit across all external-facing services (CIS 6.3, CIS 6.4); (3) Log retention policy review against NIST AU-11 — ensure retention supports the forensic lookback window Akira's dwell time requires; (4) Tabletop exercise simulating Akira's kill chain phases to validate playbook coverage for pre-encryption disruption.

NIST Phase: Post Incident

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

Controls: NIST AU-11 (Audit Record Retention), NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Implement the Event ID 1102/104 detection rule as a free Sigma rule converted to Windows Event Forwarding (WEF) subscription — WEF is built into Windows Server and forwards Security and System log events to a central collector at no cost; use the Sigma rule 'win_security_event_log_cleared.yml' from SigmaHQ as the basis. For the quarterly MFA audit, script the enumeration using 'Get-ADUser -Filter * -Properties SmartcardLogonRequired,LastLogonDate | Where-Object {$_.SmartcardLogonRequired -eq $false}' as a proxy coverage check. For the tabletop, use CISA's free Akira ransomware advisory (AA23-284A) as the scenario threat profile — it documents the exact kill chain phases observed in real intrusions and should be the scenario script baseline.

Evidence: Post-incident documentation to retain for lessons learned and regulatory purposes: (1) Full timeline of Akira dwell period reconstructed from all available log sources, annotated with MITRE ATT&CK technique IDs at each phase — this becomes the detection gap map for rule improvement; (2) Gap analysis document mapping each Akira kill chain phase against existing detection rules, showing which phases fired alerts and which were silent; (3) MFA coverage audit results showing which external-facing services were single-factor at time of initial access — this is the root cause artifact; (4) Copies of all evtx exports, WMI subscription queries, scheduled task XMLs, and memory images collected during the incident, retained per the revised AU-11 retention policy (minimum 12 months recommended given Akira's documented multi-week dwell times).

Detection Guidance

Akira's pre-encryption kill chain produces distinct log artifacts at each phase. Focus detection on these SIEM queries and alert rules:

Initial Access (T1078, T1133): Alert on authentication success from an external IP following 5+ failed attempts within 10 minutes (Windows Event IDs 4625 then 4624). Flag VPN or RDP sessions authenticated without MFA claim in the session token. Cross-reference source IPs against threat intel feeds.

Privilege Escalation (T1548, T1059): Detect cmd.exe or powershell.exe spawned by unusual parent processes (services.exe, wmiprvse.exe, mmc.exe). Alert on token impersonation API calls where supported by EDR telemetry.

Lateral Movement (T1021.002, T1047): Alert on ADMIN$ or C$ share access (Event ID 5140) originating from non-server workstations or non-standard admin hosts. Monitor WMI remote execution chains: wmiprvse.exe spawning reconnaissance or execution commands (Event ID 4688).

Reconnaissance (T1087.002, T1069.002, T1083): Detect net.exe, net1.exe, or LDAP queries enumerating domain admins or domain groups in bulk. Flag directory listing activity on file servers outside maintenance windows.

Pre-Encryption Indicator, Highest Fidelity: Windows Security log cleared (Event ID 1102) or System log cleared (Event ID 104) during a live session. This is Akira's documented pre-encryption behavior (T1070.001). Treat as a P1 incident trigger. Relevant NIST controls: AU-9 (Protection of Audit Information), SI-4 (System Monitoring). Relevant CIS safeguard: CIS 8.2 (Collect Audit Logs). Countermeasures: NIST AC-2 (Account Management), NIST SI-4 (System Monitoring).

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1057** — Process Discovery
- **T1021.002** — SMB/Windows Admin Shares
- **T1047** — Windows Management Instrumentation
- **T1548** — Abuse Elevation Control Mechanism
- **T1078.002** — Domain Accounts
- **T1087.002** — Domain Account
- **T1133** — External Remote Services
- **T1059** — Command and Scripting Interpreter
- **T1070.001** — Clear Windows Event Logs
- **T1069.002** — Domain Groups
- **T1021** — Remote Services
- **T1083** — File and Directory Discovery
- **T1486** — Data Encrypted for Impact
- **T1543.003** — Windows Service

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-6** — Configuration Settings
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1057	Process Discovery	Discovery
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1047	Windows Management Instrumentation	Execution
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1078.002	Domain Accounts	Defense-Evasion
T1087.002	Domain Account	Discovery
T1133	External Remote Services	Persistence
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1070.001	Clear Windows Event Logs	Defense-Evasion
T1069.002	Domain Groups	Discovery
T1021	Remote Services	Lateral-Movement
T1083	File and Directory Discovery	Discovery
T1486	Data Encrypted for Impact	Impact
T1543.003	Windows Service	Persistence

Sources

Source	URL	Tier
Security News	https://isc.sans.edu/diaryimages/images/fig2(1).png	T1
Vulnerability In Apache Commons Text Library	https://northwave-cybersecurity.com/threat-response/vulnerability-i...	T3
Security Notice: Apache commons-text vulnerability (CVE-2022 ...	https://support.xmatters.com/hc/en-us/articles/13843436346139-Secur...	T3
Vulnerability (Text4Shell) (CVE-2022-42889) - Cloudera Community	https://community.cloudera.com/t5/Support-Questions/Vulnerability-T...	T3
CVE-2022-42889 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2022-42889	T3

Generated 2026-05-28 06:46 UTC by TJS Security Command Center