INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

Geopolitical Convergence: State Actors, Hacktivists, and Ransomware Operators Targeting Critical Infrastructure OT/ICS Systems

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0109
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cleo Managed File Transfer Software (CVE-2024-55956, CVE-2024-50623); OT/ICS systems in energy, water, and agriculture sectors; perimeter appliances (unspecified vendors); virtualization platforms (unspecified); telecom networks (unspecified)
Published	2026-03-27
Discovery Source	Rss

Executive Summary

State-sponsored actors, state-aligned hacktivists, and ransomware operators are actively targeting the same critical infrastructure assets - energy, water, and agriculture OT/ICS environments - with some evidence of shared tool and infrastructure use. Attribution between actor categories remains deliberately obscured. Publicly disclosed vulnerabilities in perimeter-facing systems, including Cleo managed file transfer software (CVE-2024-55956, CVE-2024-50623), are the confirmed initial access vector. Organizations operating OT/ICS environments or managed file transfer platforms face compounded risk: a single unpatched perimeter appliance can serve as the entry point for actors ranging from ransomware crews to nation-state operators pursuing destructive or espionage objectives.

Technical Analysis

This campaign cluster reflects deliberate infrastructure and TTP sharing across actor categories that previously operated in distinct threat lanes. Confirmed exploitation targets Cleo Harmony, VLTrader, and LexiCom (versions prior to patches addressing CVE-2024-55956 and CVE-2024-50623). CVE-2024-55956 is a zero-day enabling unauthenticated remote code execution via the autorun directory; CVE-2024-50623 involves an unrestricted file upload and download flaw. Cl0p has been publicly attributed to Cleo exploitation activity by multiple security vendors, consistent with their prior MO against file transfer platforms (MOVEit, GoAnywhere). Vulnerability root causes span CWE-285 (improper authorization), CWE-494 (download of code without integrity

check), and CWE-693 (protection mechanism failure). Post-exploitation activity includes lateral movement (T1021), ingress tool transfer (T1105), data exfiltration over C2 channels (T1071), and lateral tool transfer (T1570). OT/ICS intrusions follow initial IT-side compromise; defenders report adversaries pivoting from perimeter file transfer systems into operational technology segments. MITRE ATT&CK techniques active across this cluster: T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1078 (Valid Accounts), T1566 (Phishing), T1588.002 (Tool acquisition), T1583/T1195 (infrastructure and supply chain staging), T1498 (Network DoS), T1486 (Data Encrypted for Impact), T1199 (Trusted Relationship). Attribution remains deliberately obscured through shared infrastructure; triage by TTP and infrastructure indicators rather than assumed actor type.

Action Checklist

1. Step 1: Containment. Immediately isolate Cleo Harmony, VLTrader, and LexiCom instances from external network access if running versions prior to the patches addressing CVE-2024-55956 and CVE-2024-50623. Block inbound connections to Cleo autorun directories at the perimeter firewall. Audit all external-facing file transfer and managed file transfer platforms for exposure; treat any unpatched instance as actively hostile until verified. Verify OT/ICS network segmentation from IT-side perimeter systems; confirm no direct routing paths exist between Cleo-adjacent hosts and OT segments.
2. Step 2: Detection. Query endpoint and network logs for unexpected writes to Cleo autorun directories, execution of unfamiliar binaries from Cleo process context, and outbound connections from Cleo hosts to non-standard destinations. Review authentication logs for valid account usage (T1078) from unexpected source IPs or outside business hours. In OT environments, check historian and engineering workstation logs for anomalous remote access sessions (T1021, T1133). Hunt for staged tools or compressed archives in Cleo working directories (T1105, T1570). Darktrace and Rapid7 have published behavioral detection signatures specific to Cleo post-exploitation; cross-reference your SIEM/EDR against those behavioral patterns.
3. Step 3: Eradication. Apply Cleo's official patches for CVE-2024-55956 and CVE-2024-50623 per Cleo's vendor advisory; confirm the installed version meets or exceeds the patched release. After patching, audit autorun directory contents and remove any unrecognized files. Rotate all credentials with access to Cleo instances and any downstream systems the Cleo host can reach. If compromise is confirmed or suspected, do not patch in place; re-image the host from a known-clean baseline before reconnecting to the network.
4. Step 4: Recovery. Validate patched Cleo instances against vendor release notes to confirm patch integrity. Monitor Cleo hosts and adjacent network segments for 30 days post-remediation using enhanced logging and anomaly detection. Verify OT/ICS segmentation controls remain intact post-incident; re-test firewall rules and DMZ isolation between IT and OT zones. Confirm no persistence mechanisms (scheduled tasks, autorun entries, new service accounts) remain on remediated hosts before restoring production file transfer operations.
5. Step 5: Post-Incident. Conduct a perimeter appliance audit across all external-facing data transfer, VPN, and remote access platforms for unpatched vulnerabilities; this campaign pattern consistently exploits perimeter systems in this class. Review OT/ICS network segmentation architecture; if IT-side compromise could have reached OT segments, treat that as a control gap requiring architectural remediation, not just a patch. Evaluate whether actor category was used as a triage filter during response; update playbooks to triage by TTP and infrastructure indicators rather than assumed actor type. Assess managed file transfer vendors against supply chain risk criteria (T1195) and confirm patching SLAs are

contractually defined.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and sector-specific ISAC (E-ISAC, WaterISAC, or Food and Ag-ISAC) if any confirmed or suspected lateral movement from the Cleo host toward OT historian servers, SCADA systems, or engineering workstations is detected, or if evidence of data staging or exfiltration from Cleo working directories is found, as both conditions trigger CISA critical infrastructure incident reporting obligations and may constitute a CIRCIA reportable incident for covered entities.
Recovery Notes	Before restoring production file transfer operations on any Cleo instance, verify the installed version hash against Cleo's published advisory and confirm all autorun directory contents match a known-clean baseline — do not rely solely on version strings on a host that may have been compromised. Monitor Cleo hosts, adjacent DMZ segments, and all OT-facing firewall rule sets for a minimum of 30 days post-remediation, given documented dwell times for state-actor campaigns targeting critical infrastructure OT environments and the realistic possibility that multiple threat actor groups accessed the same Cleo instances during the exposure window. If any OT historian, engineering workstation, or SCADA component was reachable from the Cleo host during the incident window, treat those OT assets as potentially compromised and conduct process integrity verification (comparing current setpoints and configurations against last known-good backups) before resuming automated OT operations.
Forensic Artifacts	Cleo autorun directory contents with preserved filesystem timestamps (typically C:\Program Files\Cleo\autorun\ or equivalent) — CVE-2024-55956 exploitation places attacker-controlled files here for automatic execution by the Cleo service; any file in this directory with a creation timestamp during the suspected compromise window and not matching the Cleo installation manifest is primary evidence of exploitation. | Cleo HTTP and HTTPS transaction logs (C:\Program Files\Cleo\logs\) covering the full exposure window — CVE-2024-50623 exploitation involves malformed or unauthorized file upload requests; logs will show the source IP, URI path, HTTP method, and payload size of the exploitation attempt and any subsequent attacker file staging activity. | Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled, filtered on parent processes matching Cleo executables — post-exploitation tool execution (webshells, staging utilities, credential dumpers) launched from Cleo process context will appear here and constitute direct evidence of the kill chain progression from initial access to post-exploitation. | Windows Scheduled Tasks export (`schtasks /query /fo LIST /v`) and Services registry hive (HKLM\SYSTEM\CurrentControlSet\Services) captured from Cleo hosts — ransomware and state-actor post-exploitation frameworks used in this campaign category commonly establish persistence via new scheduled tasks or services after initial access through MFT platform vulnerabilities. | Network flow or firewall log data capturing all outbound connections from Cleo host IPs during the exposure window, specifically sessions to non-file-transfer-partner destinations on ports 443, 80, 4444, 8080, or other non-standard ports — C2 beaconing from implants dropped via Cleo exploitation will appear in this data and may provide infrastructure indicators linkable to known state-actor or ransomware operator tooling documented in MITRE ATT&CK or CISA advisories.

Per-Action IR Details

Step 1: Containment — Immediately isolate Cleo Harmony, VLTrader, and LexiCom instances from external network access if running versions prior to the patches addressing CVE-2024-55956 and CVE-2024-50623. Block inbound connections to Cleo autorun directories at the perimeter firewall. Audit all external-facing file transfer and managed file transfer platforms for exposure; treat any unpatched instance as actively hostile until verified. Verify OT/ICS network segmentation from IT-side perimeter systems — confirm no direct routing paths exist between Cleo-adjacent hosts and OT segments.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: Use Windows Firewall (netsh advfirewall) or iptables to immediately block inbound TCP to Cleo's default listener ports (typically 443, 8080, 8443) and drop all outbound from the Cleo host except to defined file transfer partner IPs. Run `netstat -ano | findstr LISTENING` on each Cleo host to enumerate active listeners before blocking. For OT segmentation verification, use nmap from the Cleo host side (`nmap -sn `) to confirm no routing path exists — any response from OT-range IPs is a critical finding requiring immediate firewall rule insertion.

Evidence: Before isolating, capture a full memory image of each Cleo host using WinPmem or Magnet RAM Capture — CVE-2024-55956 exploitation via the autorun directory mechanism may load malicious modules into the Cleo process space that exist only in memory. Preserve a forensic image of the Cleo working directory tree (typically `C:\Program Files\Cleo\` and subdirectories including `autorun`, `inbox`, `outbox`) before any files are removed or overwritten. Capture a netstat snapshot (`netstat -anob > netstat_snapshot.txt`) and running process list (`tasklist /v /fo csv > processes.txt`) to document any active C2 sessions or unusual child processes spawned by Cleo before the network is cut.

Step 2: Detection — Query endpoint and network logs for unexpected writes to Cleo autorun directories, execution of unfamiliar binaries from Cleo process context, and outbound connections from Cleo hosts to non-standard destinations. Review authentication logs for valid account usage (T1078) from unexpected source IPs or outside business hours. In OT environments, check historian and engineering workstation logs for anomalous remote access sessions (T1021, T1133). Hunt for staged tools or compressed archives in Cleo working directories (T1105, T1570). Darktrace and Rapid7 have published behavioral detection signatures specific to Cleo post-exploitation; cross-reference your SIEM/EDR against those behavioral patterns.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), 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), MITRE ATT&CK T1078 (Valid Accounts), MITRE ATT&CK T1105 (Ingress Tool Transfer), MITRE ATT&CK T1021 (Remote Services), MITRE ATT&CK T1133 (External Remote Services), MITRE ATT&CK T1570 (Lateral Tool Transfer)

Compensating: Deploy Sysmon with a configuration that logs Event ID 11 (FileCreate) targeting Cleo autorun and inbox directories, Event ID 1 (Process Create) filtering on parent process matching Cleo executables (Harmony.exe, VLTrader.exe, LexiCom.exe), and Event ID 3 (Network Connection) for outbound from those parent processes. Query with PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 11 -and $_.Message -like '*autorun*'}`. For OT historian logs, query the OSIsoft PI or Wonderware event journal for remote session initiations outside defined maintenance windows using vendor-native query tools. Use Sigma rule `proc_creation_win_cleo_suspicious_child.yml` (community Sigma repository) adapted to Cleo process names for offline log grep if no SIEM is available: `grep -E '(Harmony|VLTrader|LexiCom)\.exe' sysmon.log | grep -v 'expected_child_process'`.

Evidence: Collect Windows Security Event Log Event ID 4688 (Process Creation) filtered on processes with parent image path matching Cleo installation directory — any cmd.exe, powershell.exe, wscript.exe, or certutil.exe spawned from Cleo context is high-confidence exploitation evidence for CVE-2024-55956. Pull IIS or Cleo's own HTTP access logs (typically at `C:\Program Files\Cleo\logs\`) and search for POST requests to autorun-adjacent endpoints with

non-standard User-Agent strings or oversized payloads indicative of the file upload exploitation path in CVE-2024-50623. On OT historian and engineering workstations, extract RDP or VNC session logs (Windows Security Event IDs 4624/4625 with Logon Type 10) and cross-reference source IPs against the Cleo host's known IP — lateral movement from a compromised Cleo host to OT-adjacent systems would appear here first.

Step 3: Eradication — Apply Cleo's official patches for CVE-2024-55956 and CVE-2024-50623 per Cleo's vendor advisory; confirm the installed version meets or exceeds the patched release. After patching, audit autorun directory contents and remove any unrecognized files. Rotate all credentials with access to Cleo instances and any downstream systems the Cleo host can reach. If compromise is confirmed or suspected, do not patch in place — re-image the host from a known-clean baseline before reconnecting to the network.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management), 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), CIS 5.2 (Use Unique Passwords)

Compensating: Before re-imaging, use ClamAV with an updated signature database to scan the full Cleo installation directory and any directories reachable by the Cleo service account: `clamscan -r --log=clamav_scan.txt 'C:\Program Files\Cleo\'`. Use PowerShell to enumerate and hash all files in the autorun directory against a known-clean Cleo installation manifest: `Get-FileHash -Algorithm SHA256 (Get-ChildItem -Recurse 'C:\Program Files\Cleo\autorun\') | Export-Csv autorun_hashes.csv`. For credential rotation without a PAM tool, use the Windows Local Security Policy or Active Directory to force password reset on all accounts that authenticated to the Cleo host since the earliest suspected compromise date (pull from Security Event ID 4624 logs). Re-image from a vendor-provided or organizationally-maintained offline golden image, not from a snapshot taken after the vulnerability was publicly disclosed (post-December 2024).

Evidence: Before eradicating, preserve the full contents of the Cleo autorun directory as a forensic zip with preserved timestamps (`robocopy /COPYALL /LOG` or `tar --preserve-permissions`) — malicious files dropped via CVE-2024-55956 exploitation are placed here and represent primary forensic evidence of the initial access stage. Capture the Windows registry hive `HKLM\SYSTEM\CurrentControlSet\Services` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` from the Cleo host to identify any persistence mechanisms (new services or autorun entries) installed by post-exploitation tooling before eradication removes them. Extract and preserve Cleo's internal transaction and session logs from `C:\Program Files\Cleo\logs\` — these logs record file transfer partner sessions and may identify exfiltration activity or the attacker's originating IP used during the exploitation of CVE-2024-50623.

Step 4: Recovery — Validate patched Cleo instances against vendor release notes to confirm patch integrity. Monitor Cleo hosts and adjacent network segments for 30 days post-remediation using enhanced logging and anomaly detection. Verify OT/ICS segmentation controls remain intact post-incident; re-test firewall rules and DMZ isolation between IT and OT zones. Confirm no persistence mechanisms (scheduled tasks, autorun entries, new service accounts) remain on remediated hosts before restoring production file transfer operations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CM-6 (Configuration Settings), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify Cleo patch integrity by comparing the SHA-256 hash of the installed Cleo binary against the hash published in Cleo's official vendor advisory — do not trust the version string alone, as a compromised host may report incorrect version data. Use Sysmon Event ID 7 (Image Load) during the first 72 hours post-recovery to detect any DLL hijacking attempts against the newly patched Cleo process. For OT segmentation re-validation without a

commercial network scanner, use a controlled test: from a known IT-side host, attempt ICMP and TCP connections to OT historian and engineering workstation IPs (`Test-NetConnection -ComputerName -Port 102` for Siemens S7, port 44818 for EtherNet/IP) — any successful connection is a segmentation failure requiring immediate firewall remediation. Audit scheduled tasks with `schtasks /query /fo LIST /v > schtasks_audit.txt` and new service accounts with `net user` and `wmic useraccount list brief` before restoring production traffic.

Evidence: During the 30-day enhanced monitoring window, collect and retain all Cleo HTTP access logs, Sysmon Event ID 1 and 3 logs, and Windows Security Event IDs 4624/4625/4688 from Cleo hosts — given the multi-actor nature of this campaign (state actors, hacktivists, ransomware operators), a second-wave access attempt by a different threat actor using the same initial access vector (Cleo autorun abuse) during recovery is a realistic scenario and must be detectable from retained logs. Capture baseline file hashes of all files in the Cleo installation and working directories immediately post-recovery using `Get-FileHash` and store offline — any deviation detected during the monitoring period indicates re-compromise or residual persistence. For OT environments, pull and preserve historian data trend logs covering the incident window, as manipulated setpoints or process anomalies caused by actor access to OT-adjacent systems may only become apparent during post-recovery operational comparison.

Step 5: Post-Incident — Conduct a perimeter appliance audit across all external-facing data transfer, VPN, and remote access platforms for unpatched vulnerabilities; this campaign pattern consistently exploits perimeter systems in this class. Review OT/ICS network segmentation architecture — if IT-side compromise could have reached OT segments, treat that as a control gap requiring architectural remediation, not just a patch. Evaluate whether actor category was used as a triage filter during response; update playbooks to triage by TTP and infrastructure indicators, not assumed actor type. Assess managed file transfer vendors against supply chain risk criteria (T1195) and confirm patching SLAs are contractually defined.

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 RA-3 (Risk Assessment), NIST SA-12 (Supply Chain Protection), NIST SI-2 (Flaw Remediation), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), MITRE ATT&CK T1195 (Supply Chain Compromise)

Compensating: Use CISA's Known Exploited Vulnerabilities (KEV) catalog as the authoritative baseline for the perimeter appliance audit — cross-reference every external-facing appliance (MFT platforms, VPN concentrators, remote access gateways) against the KEV list using a spreadsheet mapping asset inventory to CVE IDs; any KEV match with no confirmed patch date is an immediate remediation priority. For OT/ICS segmentation architectural review, use the ICS-CERT/CISA Architecture Review Service request process (free for critical infrastructure operators) or apply NIST SP 800-82 Rev. 3 DMZ design guidance to evaluate whether the Cleo-adjacent IT segment had any permitted routing to OT historian, SCADA server, or engineering workstation subnets. For MFT vendor supply chain assessment, request a Software Bill of Materials (SBOM) from Cleo and any other MFT vendors and review third-party component CVE exposure using the free OWASP Dependency-Check tool against the disclosed component list.

Evidence: Compile the full timeline of Cleo access logs, authentication events, and autorun directory write events spanning the entire suspected compromise window (not just the confirmed incident date) — given that this campaign involves converging state-actor and ransomware operators who may have maintained persistent access for extended periods before detection, the actual dwell time may significantly predate the first alert. Preserve all indicators of compromise (IOCs) collected during the investigation — file hashes from autorun directory artifacts, observed C2 IP addresses from Cleo outbound connection logs, and any novel Cleo-process child process command lines — and submit to CISA's Automated Indicator Sharing (AIS) program or your ISAC (E-ISAC for energy, WaterISAC for water) to support sector-wide defense against this multi-actor campaign. Document the specific triage decisions made during response, particularly any actor-attribution assumptions that influenced containment timing, and incorporate into an updated OT/ICS incident response playbook that leads with TTP-based triage (MITRE ATT&CK technique correlation) rather than actor-category assumptions.

Detection Guidance

Priority detection signals: (1) File creation events in Cleo autorun directories from non-Cleo processes or at unexpected times, Windows Event ID 4663 or equivalent EDR file write telemetry. (2) Cleo process spawning cmd.exe, powershell.exe, or wscript.exe, parent-child process anomaly in EDR. (3) Outbound HTTP/HTTPS from Cleo host IPs to destinations not in the approved transfer partner list, filter in proxy or firewall logs. (4) Authentication events using service or application accounts from external IPs (T1078), query identity provider or Windows Security Event ID 4624/4625 with logon type 3 or 10. (5) Large data transfers or compressed file staging in Cleo working directories shortly before outbound connections, correlate DLP or file activity monitoring with network flow data. (6) In OT environments: new or unexpected remote sessions to engineering workstations or historian servers, especially originating from IT-segment hosts adjacent to Cleo. Behavioral context: Cl0p and similar operators typically move quickly from initial access to exfiltration; dwell time before data staging is often under 48 hours in file transfer platform compromises. Prioritize retrospective log review covering the 30 days prior to detection.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Cleo autorun directory paths (platform-specific, see Cleo vendor advisory)`	Adversaries write malicious files to Cleo autorun directories to achieve code execution on vulnerable instances of Harmony, VLTrader, and LexiCom	HIGH
URL	`No discrete network IOCs confirmed in source material reviewed`	Specific IP addresses, domains, and file hashes associated with this campaign cluster were not included in the source data provided. Consult Rapid7, Darktrace, and Cybereason published advisories directly for current IOC lists; treat any IOCs as time-limited given confirmed infrastructure rotation by threat actors in this cluster.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1498** — Network Denial of Service
- **T1566** — Phishing
- **T1021** — Remote Services
- **T1588.002** — Tool
- **T1570** — Lateral Tool Transfer
- **T1105** — Ingress Tool Transfer
- **T1071** — Application Layer Protocol

- **T1583** — Acquire Infrastructure
- **T1195** — Supply Chain Compromise
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1199** — Trusted Relationship

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
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **AC-20** — Use of External Systems
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5**
- **2.6**

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1498	Network Denial of Service	Impact
T1566	Phishing	Initial-Access
T1021	Remote Services	Lateral-Movement
T1588.002	Tool	Resource-Development
T1570	Lateral Tool Transfer	Lateral-Movement
T1105	Ingress Tool Transfer	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1195	Supply Chain Compromise	Initial-Access
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/we-are-at-war.html	T3
Cleo File Transfer Vulnerability: Patch Pitfalls and ... - Darktrace	https://www.darktrace.com/blog/cleo-file-transfer-vulnerability-pat...	T3
Widespread Exploitation of Cleo File Transfer Software | Rapid7 Blog	https://www.rapid7.com/blog/post/2024/12/10/etr-widespread-exploita...	T3
Cleo releases CVE for actively exploited flaw in file-transfer software	https://www.cybersecuritydive.com/news/cleo-exploited-flaw-file-tra...	T3
CVE-2024-55956: Zero-Day Vulnerability in Cleo Software Could ...	https://www.cybereason.com/blog/cve-2024-55956-cleo-vulnerability	T3

Generated 2026-03-29 18:33 UTC by TJS Security Command Center