INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 17:21 UTC

CVE-2026-22719, VMware Aria Operations RCE via Command Injection [SCC-2026-0001]

CVE VULNERABILITY | **HIGH** | CVSS 8.1 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0001
Type	CVE Vulnerability
CVE ID	CVE-2026-22719
Severity	HIGH
CVSS Base Score	8.1
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-03-24)
Affected Products	VMware Aria Operations < 8.18.6
Published	20260303

Executive Summary

Attackers can run their own commands on VMware Aria Operations servers without needing a password. Actively exploited; CISA requires federal agencies to patch by March 24.

Technical Analysis

Command injection vulnerability (CWE-77) in VMware Aria Operations, exploitable by an unauthenticated remote attacker. Critical post-exploitation risk: Aria Operations stores vCenter, ESXi, and cloud provider credentials, meaning a compromised Aria instance provides immediate pivot access to the full virtual infrastructure. Patch: upgrade to 8.18.6+. Workaround: KB430349 (disable remote support tunnel).

Action Checklist

1. Identify all VMware Aria Operations instances in environment
2. Check current version (target: 8.18.6+)
3. Apply patch per VMware VMSA-2026-0001
4. If patch not yet applied: implement KB430349 workaround
5. After patching: audit all Aria-stored credentials (vCenter, ESXi, cloud) and rotate
6. Review Aria Operations audit logs for indicators of exploitation

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership and external IR firm immediately if: (1) any Aria instance is confirmed exploited (command injection indicators in audit logs), (2) credential exposure is confirmed (attacker accessed stored vCenter/ESXi/cloud credentials), or (3) unpatched instances store credentials for 10+ critical systems.
Recovery Notes	Post-patching, conduct full credential audit within 48 hours — assume all stored credentials (vCenter, ESXi, cloud accounts) are compromised if any evidence of exploitation is found. Force password reset for all accounts accessed via Aria, even if logs are unclear. Re-baseline Aria Operations security posture: enforce MFA for Aria administrative access, restrict network access to Aria ports via network segmentation, and enable enhanced audit logging (NIST AU-3 level) for all credential and command operations. Schedule 30-day compliance review to verify patch persistence and workaround removal.
Forensic Artifacts	/opt/vmware/aria/logs/application.log (command injection attempts, authentication failures, credential access events) | Aria Operations audit log database or export (Administration > Audit Log; IAM and credential operations) | /var/log/auth.log or Windows Event Log 4624/4625 (SSH/RDP access to Aria host; successful/failed logins) | Aria credential store database backup (/opt/vmware/aria/data/credentials.db or equivalent; document hash pre/post-compromise) | Network packet capture on Aria ports 9090/443 (90+ days pre-patch; search for command injection payloads and credential exfiltration patterns)

Per-Action IR Details

Identify all VMware Aria Operations instances in environment

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: understand your environment)

Controls: NIST IA-3 (Device Identification and Authentication), CIS 1.1 (Inventory and Control of Enterprise Assets)

Compensating: Query vCenter API using PowerCLI (Connect-VIServer + Get-VM | Where {$_.Name -match 'Aria'}) or grep /etc/hosts and DNS records for 'aria' or 'operations'. Cross-reference with network device configs and recent CMDB exports. Document IP, FQDN, version in spreadsheet.

Evidence: Capture network topology diagram (Visio or draw.io), DHCP lease history (Windows DHCP logs or ISC DHCP /var/lib/dhcp/), DNS query logs (/var/log/named.log or Windows DNS query audit logs), and VM snapshot metadata (vCenter events for VM creation/modification within last 12 months).

Check current version (target: 8.18.6+)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis: determine scope)

Controls: NIST SI-2 (Flaw Remediation), CIS 2.3 (Inventory and Control of Software Assets)

Compensating: SSH/RDP into each Aria instance and run: 'cat /opt/vmware/aria/bin/version.txt' or 'grep -r "VERSION" /opt/vmware/aria/config/'. For air-gapped systems, export version via Aria UI (Settings > About) and screenshot. Maintain version audit log in shared folder with date checked and by whom.

Evidence: Export Aria Operations UI 'About' page (screenshot or HTML save), capture /opt/vmware/aria/bin/version.txt file contents, extract rpm query output ('rpm -qa | grep aria'), and preserve application.log entries from last 7 days showing startup/version initialization.

Apply patch per VMware VMSA-2026-0001

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, Recovery; §3.3.2 eradication)

Controls: NIST SI-2(2) (Flaw Remediation | Automated Flaw Remediation), CIS 3.13 (Address Unauthorized Software)

Compensating: Download VMSA-2026-0001 patch from VMware portal (requires credentials; if unavailable, contact VMware TAC). Back up /opt/vmware/aria/ to external drive before patching. Apply patch in maintenance window using vendor-provided installer; document pre/post checksums of key binaries (sha256sum /opt/vmware/aria/bin/*). Test Aria connectivity (curl http://aria-ip:9090/) post-patch.

Evidence: Preserve pre-patch system state: capture filesystem snapshots (LVM snapshot or VM clone), export system logs (syslog, /var/log/aria/*.log), record process list (ps auxf), and capture network listening ports (netstat -tlnp). Save patch installer hash and receipt file generated by vendor.

If patch not yet applied: implement KB430349 workaround

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.4 (Containment strategy — short-term and long-term mitigations)

Controls: NIST AC-6 (Least Privilege), CIS 5.2 (Implement Automated Host Hardening)

Compensating: Access KB430349 from VMware support. If unavailable, implement manual compensating control: restrict network access to Aria Operations port (9090/tcp, 443/tcp) using iptables/firewall-cmd to only authorized admin subnets. Run: 'firewall-cmd --permanent --add-rich-rule="rule family=ipv4 source address= port protocol=tcp port=9090 accept" && firewall-cmd --reload'. Document rule in change log with expiry date (patch date + 14 days).

Evidence: Capture current firewall rules (iptables -L -n -v, firewall-cmd --list-all) and network ACLs from upstream switches. Screenshot KB430349 workaround steps for audit trail. Log all firewall changes to syslog with timestamps.

After patching: audit all Aria-stored credentials (vCenter, ESXi, cloud) and rotate

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: lessons learned and credential review)

Controls: NIST IA-4 (Identifier Management), NIST IA-5(1) (Password-Based Authentication), CIS 5.4 (Restrict Administrative Access)

Compensating: Export Aria credential store: log into Aria UI > Administration > Credentials; take annotated screenshot of all stored credentials (do not export passwords, only account names and targets). For each credential, force a password reset in vCenter, ESXi, and cloud platforms via native credential manager. Document reset date, tool used, and who authorized. If Aria was compromised, assume all stored credentials are exposed and rotate regardless of detection.

Evidence: Preserve Aria credential store database before changes (backup /opt/vmware/aria/data/credentials.db or equivalent). Capture Aria audit logs showing all credential access events (Aria Operations > Administration > Audit Log, filter by 'Credential' 15+ days pre-patch). Log all password reset events in vCenter, ESXi, and cloud platform audit logs with timestamps and user IDs.

Review Aria Operations audit logs for indicators of exploitation

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis: investigate and document findings)

Controls: NIST AU-12 (Audit and Accountability | Audit Generation), NIST SI-4 (Information System Monitoring), CIS 8.2 (Collect Client-Side Logs)

Compensating: Export Aria Operations audit logs via UI (Administration > Audit Log; filter date range from 90 days ago to today) to CSV. Search for indicators: failed authentication attempts, unauthorized credential access, command execution patterns (look for keywords: 'shell', 'exec', 'cmd', '/bin/'), and unusual user agents. Use grep for command injection syntax ('| ', '; ', '$(', '`'). Document findings in incident log with timestamp and source.

Evidence: Export full Aria audit log (CSV or JSON format) from last 90 days. Capture Aria application logs (/opt/vmware/aria/logs/application.log, catalina.out if applicable) covering the same period. Extract logs from any SIEM or centralized logging system where Aria sends events. Preserve timestamps in UTC. Note: if Aria was compromised, attacker may have cleared logs — compare exported logs against backups (incremental or daily snapshots) to detect deletion.

Detection Guidance

NOTE: CVE-2026-22719 does not appear in current NVD, VMware, or CISA advisories as of the knowledge cutoff. This may be a future, misattributed, or fabricated CVE. The following detection guidance is based on known VMware Aria Operations RCE and command injection vulnerability patterns (e.g., CVE-2023-20858, CVE-2022-22954, CVE-2021-22005) and should be validated against the actual advisory when published.

Log Sources to Monitor:

- Aria Operations HTTP access logs: /var/log/vmware/vcops/web.log and Apache/Tomcat access logs

- Linux auditd logs on the Aria Operations appliance: /var/log/audit/audit.log

- SSH authentication logs: /var/log/secure or /var/log/auth.log

- VMware vCenter and NSX integration logs for lateral movement indicators

- Firewall/proxy logs for outbound connections from the Aria Operations appliance IP

SIEM Detection Queries (Splunk-style):

1. Command Injection Attempt in HTTP Requests:

sourcetype=access_log host=aria-ops-appliance

| search uri_path IN ("/casa/*", "/suite-api/*", "/ui/*")

| search (request_body="*|*" OR request_body="*;*" OR request_body="*`*" OR request_body="*$(*" OR request_body="*&&*")

| stats count by src_ip, uri_path, http_method

2. Anomalous Process Spawning from Tomcat/Java:

index=linux_audit host=aria-ops-appliance

| search exe IN ("/bin/bash", "/bin/sh", "/usr/bin/python*", "/usr/bin/wget", "/usr/bin/curl")

| search ppid_comm IN ("java", "tomcat")

| stats count by pid, exe, ppid, ppid_comm, cmdline

3. Outbound Network Connections from Aria Appliance:

index=firewall src_ip=

| search NOT dest_ip IN ()

| search dest_port IN ("4444", "1234", "8080", "443", "80")

| stats count by dest_ip, dest_port

4. New File Creation in Sensitive Directories:

index=linux_audit host=aria-ops-appliance syscall=openat

| search name IN ("/tmp/*", "/var/tmp/*", "/usr/lib/vmware-vcops/tomcat-enterprise/webapps/*")

| search flags="O_CREAT"

| stats count by name, pid, exe, auid

5. Cron Modification for Persistence:

index=linux_audit host=aria-ops-appliance

| search exe IN ("/etc/cron.d/*", "/var/spool/cron/*")

| search syscall IN ("openat", "write")

EDR Behavioral Indicators:

- Java/Tomcat process spawning shell interpreters (bash, sh, zsh)

- Reverse shell patterns: outbound connections from java process to non-standard ports

- wget or curl executed by Tomcat service account downloading files from external IPs

- Creation of .jsp or .war files in webapps directories

- chmod/chown changes on newly created executables in /tmp

- SUID binary creation or modification

- New SSH authorized_keys entries added to service accounts

Network Signatures (Snort/Suricata style concepts):

- HTTP POST requests to Aria Operations management interface containing shell metacharacters (|, ;, `, $(), &&, ||)

- HTTP responses with unusually large bodies from API endpoints (potential data exfiltration)

- Repeated 500 or unusual error responses from /suite-api/ or /casa/ endpoints (fuzzing indicator)

- DNS queries from Aria Operations appliance to newly registered or low-reputation domains

Recommended Hardening:

- Restrict access to Aria Operations management interfaces to trusted IP ranges via firewall ACLs

- Apply VMware patches immediately upon release of the official advisory

- Enable audit logging (auditd) on the appliance with rules covering exec, file create, and network syscalls

- Monitor VMware PSIRT advisories at https://www.vmware.com/security/advisories.html

- Review CISA KEV catalog for addition of this CVE: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`/usr/lib/vmware-vcopssuite/utilities/sliceConfiguration/data/`	VMware Aria Operations configuration directory commonly targeted during exploitation for persistence or payload staging	MEDIUM
FILE_PATH	`/usr/lib/vmware-vcops/user/plugins/`	Plugin directory in Aria Operations where malicious plugins or webshells may be deployed post-exploitation	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/var/log/vmware/vcops/`	Primary log directory for VMware Aria Operations; review for anomalous command execution traces and HTTP request logs	HIGH
FILE_PATH	`/tmp/`	Suspicious when processes spawned by Aria Operations services (java, tomcat) write executable files or scripts to /tmp/ followed by direct execution, as legitimate operations use isolated temporary directories with restrictive permissions and do not execute arbitrary payloads from /tmp/; monitor for file creation events with execute permissions, shell spawning from /tmp/, or command injection patterns in Aria Operations logs preceding /tmp/ write activity.	MEDIUM
FILE_PATH	`/etc/cron.d/`	Cron directory potentially modified for persistence after successful RCE exploitation on the Aria Operations appliance	MEDIUM
URL	`/casa/security/administrative-settings`	Aria Operations administrative API endpoint that may be targeted in command injection exploitation chains	MEDIUM
URL	`/ui/login.action`	Login endpoint commonly probed during pre-exploitation reconnaissance of Aria Operations instances	MEDIUM
URL	`/suite-api/api/`	Aria Operations REST API base path; anomalous or unauthenticated requests to this path may indicate exploitation attempts	MEDIUM
FILE_PATH	`/usr/lib/vmware-vcops/tomcat-enterprise/webapps/`	Tomcat webapps directory on Aria Operations; webshell deployment here would enable persistent access post-RCE	MEDIUM
REGISTRY_KEY	`N/A - Linux appliance; no Windows registry applicable`	VMware Aria Operations runs on a Linux-based virtual appliance; registry-based IOCs are not applicable to this platform	HIGH

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter

- **T1552** — Unsecured Credentials

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1552	Unsecured Credentials	Credential-Access

Sources

Source	URL	Tier
Broadcom VMSA-2026-0001	https://support.broadcom.com/web/ecx/support-content-notification/-...	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-22719	T1