EnCyb

Severity: High

Advisory Type: Security

VMware Aria Operations RCE & Privilege Escalation

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Three vulnerabilities (CVE-2026-22719, CVE-2026-22720, CVE-2026-22721) in VMware Aria Operations may allow command injection (leading to remote code execution), stored XSS, and privilege escalation. The most critical flaw (CVSS 8.1) affects migration workflows and could lead to full system compromise, particularly in VMware Cloud Foundation and Telco Cloud environments. Organizations using affected 8.x versions should urgently upgrade to patched releases (8.18.6 / 9.0.2.0).

- CVE: CVE-2026-22719, CVE-2026-22720, CVE-2026-22721
- CVSS: 8.1 (Command Injection), 8.0 (Stored XSS), 6.2 (Privilege Escalation)
- Active Region: Global
- Affected Sector: Multiple sectors
- Affected Product: VMware Aria Operations (including Cloud Foundation and Telco Cloud deployments)
- Severity: High
- Published Date: February 24, 2026

TECHNICAL DETAILS

- **Target:** VMware Aria Operations management plane, specifically the migration workflows and custom benchmark functionality that are accessible within enterprise and telco cloud deployments.

- **Root Cause:** The vulnerabilities stem from improper input validation enabling command injection during migration workflows, insufficient output encoding allowing stored cross-site scripting through custom benchmarks, and improper privilege boundary enforcement between vCenter-integrated roles and Aria Operations administrative controls, leading to privilege escalation.

- **Prerequisite for Exploitation:** Exploitation requires network access to a system undergoing migration for the command injection flaw (no prior authentication required), authenticated access with benchmark creation privileges for the stored XSS issue, and authenticated vCenter-level access in integrated environments for the privilege escalation vulnerability.

AFFECTED PRODUCTS & VERSION

- VMware Cloud Foundation vSphere Foundation Operations 9.x.x.x

- VMware Aria Operations 8.x
- VMware Cloud Foundation 5.x / 4.x (bundled VMware Aria Operations)
- VMware Telco Cloud Platform 5.x / 4.x
- VMware Telco Cloud Infrastructure 3.x / 2.x

FIXED VERSIONS

- VMware Cloud Foundation / vSphere Foundation Operations 9.0.2.0
- VMware Aria Operations 8.18.6
- VMware Cloud Foundation 5.x / 4.x – Refer to KB92148
- VMware Telco Cloud Platform 5.x / 4.x – Refer to KB428241
- VMware Telco Cloud Infrastructure 3.x / 2.x – Refer to KB428241

IMPACT

- Remote code execution via command injection during migration workflows.
- Administrative session compromise via stored XSS.
- Privilege escalation from vCenter access to full Aria Operations administrative control.
- Potential compromise of cloud control planes and monitoring systems.
- Elevated risk of lateral movement across hybrid environments.
- Unauthorized configuration changes impacting service integrity and availability.

RECOMMENDATIONS

- Immediately upgrade all affected deployments to the latest fixed versions.
- Inventory and verify all Aria Operations instances across environments.
- Restrict and monitor migration workflows until remediation is complete.
- Review RBAC mappings and enforce least-privilege access controls.
- Conduct a post-patch security review to validate system integrity.

REFERENCE

- https://cyberpress.org/multiple-vmware-aria-vulnerabilities/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com