# VMware Aria Operations Vulnerabilities Could Allow Command Execution and Privilege Escalation

**TL;DR**

*Broadcom published updates for VMware Aria Operations and addressed three vulnerabilities that could allow command execution, cross-site scripting, and privilege escalation within the platform.*

*One vulnerability (CVE-2026-22719) could allow an unauthenticated attacker to execute commands during migration processes and has reported (but unconfirmed) activity in the wild.*

## Overview

There are vulnerabilities (CVE-2026-22719, CVE-2026-22720, and CVE-2026-22721) in VMware Aria Operations. The vulnerabilities affect infrastructure monitoring and operations management environments.

### Affected Products

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

**CVE-2026-22719** (CVSS 8.1)

- The most serious vulnerability is CVE-2026-22719 and is a command injection vulnerability. An unauthenticated attacker could exploit this flaw during support-assisted migration processes to execute arbitrary commands on the system running VMware Aria Operations. Successful exploitation could lead to remote code execution. Broadcom has acknowledged reports that this vulnerability may already be exploited in the wild, though the company has not independently confirmed those reports.

**CVE-2026-22720** (CVSS 8.0)

- This is a stored cross-site scripting (XSS) vulnerability. An attacker with permissions to create custom benchmarks within Aria Operations could inject malicious scripts. Those scripts could execute when viewed by administrators, allowing the attacker to perform actions within the interface using the victim's privileges.

**CVE-2026-22721** (CVSS 6.2)

- This vulnerability allows privilege escalation. An attacker who already has access to Aria Operations through **VMware vCenter integration** could exploit this vulnerability to gain administrative privileges within the platform.

Because VMware Aria Operations provides centralized monitoring and visibility into virtual infrastructure environments, attackers who gain access to the platform could obtain valuable information about systems, configurations, and infrastructure health across an organization. Aspire recommends patching immediately.

## Aspire Protects

- **Patch** - Apply the latest security updates:
  - VMware Aria Operations 8.18.6
  - VMware Cloud Foundation Operations 9.0.2.0
  - See Broadcom's advisory for more information.
- Restrict access to administrative functions and custom benchmark creation within Aria Operations.
- Monitor logs and system activity within VMware infrastructure for unexpected commands or administrative actions.
- Review permissions between vCenter and Aria Operations integrations to ensure only authorized accounts have access.

### TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit the VMware Aria Operations command injection vulnerability to execute arbitrary commands on the underlying system.

Execution

- Command and Scripting Interpreter: Unix Shell [T1059.004] – After exploiting the vulnerability, the attacker may run system-level commands on the host.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit the privilege escalation vulnerability to obtain administrative access within VMware Aria Operations.

### IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

### Targeted Industries

Organizations that rely on VMware-based virtualization infrastructure and centralized monitoring platforms may be impacted, including:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

## Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**

- The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Supporting Documentation

Support Content Notification - Support Portal - Broadcom support portal