# VMware Aria Operations and VMware Tools - Privilege Escalation Vulnerability

**TL;DR**

*VMware released patches for three vulnerabilities in Aria Operations and VMware Tools, including a local privilege escalation flaw (CVE-2025-41244) that Broadcom confirmed may already be exploited in the wild.*

*The vulnerabilities could allow attackers to gain root access on virtual machines, expose user credentials, or access other guest systems.*

## Overview

Broadcom released updates for multiple vulnerabilities affecting VMware Aria Operations and VMware Tools. The most serious issue, CVE-2025-41244 (CVSS 7.8), allows a local user with limited privileges on a VM to elevate privileges to root. Broadcom's advisory states that the vulnerability may have been exploited in the wild. The other two vulnerabilities, CVE-2025-41245 (information disclosure, CVSS 4.9) and CVE-2025-41246 (improper authorization, CVSS 7.6), could allow credential theft or unauthorized access across guest VMs.

### Affected Products

- VMware Aria Operations (8.x)
- VMware Tools (11.x – 13.x on Windows and Linux)
- VMware Cloud Foundation (4.x – 9.x)
- VMware Telco Cloud Platform (4.x – 5.x)
- VMware Telco Cloud Infrastructure (2.x – 3.x)

### Vulnerability Breakdown

- **CVE-2025-41244 – Local Privilege Escalation**
  A local user with non-admin rights on a VM running VMware Tools and managed through Aria Operations (with SDMP enabled) can exploit this flaw to gain root access. This could allow full system control and potential lateral movement across the environment. No workaround is available.

- **CVE-2025-41245 – Information Disclosure**
  An attacker with standard user privileges in Aria Operations can exploit this flaw

to reveal credentials belonging to other users. This exposure could allow further unauthorized access or account takeover within the platform.

- **CVE-2025-41246 – Improper Authorization**
  VMware Tools for Windows fails to enforce proper access controls, allowing an authenticated attacker to access other guest VMs when they already possess valid credentials for both vCenter/ESX and the targeted VMs. This issue affects only Windows guests.

Active exploitation of CVE-2025-41244 puts VMware environments in a vulnerable position. A local privilege escalation in guest VMs can quickly lead to full system compromise if attackers move laterally into vCenter or other hosts. Organizations running VMware Tools on Windows systems should patch immediately.

## Aspire Protects

- **Patch** - Apply the latest patches immediately for VMware Aria Operations 8.18.5, VMware Tools 12.5.4 and 13.0.5, and Cloud Foundation 9.0.1.0. See Broadcom's advisory for further information.
- Confirm that all guest systems running VMware Tools have been updated, especially Windows VMs.
- Review privilege assignments and disable unnecessary local accounts with administrative access.
- Monitor for signs of privilege escalation or unexpected guest-to-guest activity within vCenter environments.

**TTPs to Watch**

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker may exploit local vulnerabilities to gain root or administrator privileges on a VM.

Credential Access

- Credential Dumping [T1003] – The attacker may attempt to retrieve user credentials exposed through Aria Operations.

Lateral Movement

- Remote Services [T1021] – An attacker who gains elevated privileges may attempt to access additional VMs via shared infrastructure.

Discovery

- System Information Discovery [T1082] – The attacker may enumerate system configurations to identify exploitable paths within the VMware environment.

**IoCs**

There are no known IoCs associated with the above vulnerabilities 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**

These vulnerabilities impact organizations that depend on VMware-based infrastructure, including:

- Manufacturing
- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology

## Aspire's 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