VMware Aria Automation SSRF Vulnerability

Overview

VMware has released an update to address a server-side request forgery (SSRF) vulnerability (CVE-2025-22215) in VMware Aria Automation. This vulnerability has a CVSS score of 4.3. The issue allows an attacker with "Organization Member" access to enumerate internal services within the host or network.

CVE-2025-22215 is a server-side request forgery (SSRF) vulnerability that could allow an attacker to enumerate internal services running on the host or connected network.

Failure to patch this vulnerability could allow attackers with valid credentials to identify internal services or resources, which may allow for further exploitation or unauthorized access. This could lead to compromised data integrity and potential lateral movement within the network.

Aspire Protects

- **Patch –** There are no workarounds, making patching the only solution. Please see VMware's advisory for patch guidance.
    - VMware Aria Automation - Update to version 8.18.1 patch 1.
    - VMware Cloud Foundation - Refer to KB 385294 for patch details.

TTPs to Watch

Discovery

- Network Service Scanning (T1046) – The attacker may attempt to discover and map internal services or hosts using crafted requests.

IoCs

There are no known IoCs associated with CVE-2025-22215 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

This VMware vulnerability could impact a range of industries that rely on VMware Aria Automation for IT automation and infrastructure management. Key industries include:

- Technology and IT Services
- Retail
- Financial Services
- Healthcare
- Education
- And others

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

NVD - CVE-2025-22215

Support Content Notification - Support Portal - Broadcom support portal

VMware Aria Automation 8.18.1 Cumulative Update - Patch 1