VMware Aria Operations and Aria Operations for Logs Vulnerabilities

Overview

VMware has released security updates addressing multiple vulnerabilities in VMware Aria Operations and VMware Aria Operations for Logs. These flaws, tracked as CVE-2025-22218 through CVE-2025-22222, impact VMware Cloud Foundation as well.

Exploitation of these vulnerabilities could lead to information disclosure, privilege escalation, and cross-site scripting (XSS) attacks.

Vulnerability Breakdown

CVE-2025-22218 (Information Disclosure) – CVSS 8.5

- An attacker with View Only Admin permissions could read credentials of VMware products integrated with Aria Operations for Logs.
- Impact – Compromised credentials may be leveraged to access sensitive systems.
- Fix – Update to version 8.18.3.

CVE-2025-22219 (Stored Cross-Site Scripting) – CVSS 6.8

- An attacker inject malicious scripts that execute with admin privileges.
- Impact – Potential for unauthorized operations and data exposure.
- Fix – Update to version 8.18.3.

CVE-2025-22220 (Broken Access Control) – CVSS 4.3

- An attacker with network access may exploit the API to perform admin-level actions.
- Impact – Unauthorized privilege escalation.
- Fix – Update to version 8.18.3.

CVE-2025-22221 (Stored Cross-Site Scripting) – CVSS 5.2

- An attacker may inject scripts that execute when deleting agent configurations.
- Impact – Potential for browser-based exploitation.
- Fix – Update to version 8.18.3.

CVE-2025-22222 (Information Disclosure) – CVSS 7.7

- An attacker could retrieve credentials for outbound plugins if a valid service credential ID is known.
- Impact – Exposure of credentials that could be used in further attacks.
- Fix – Update to version 8.18.3.

These vulnerabilities impact the following products:

- VMware Aria Operations for Logs (versions 8.x)
- VMware Aria Operations (versions 8.x)
- VMware Cloud Foundation (versions 5.x, 4.x)

Organizations should apply the VMware update immediately to prevent exploitation. Delaying patches increases the risk of attackers taking full control of VMware environments.

Aspire Protects

- **Patch –** Apply the 8.18.3 update for all affected products. Please see Broadcom's advisory for patch guidance.
- Limit user access where possible to reduce risk.

TTPs to Watch

Credential Access
- Unsecured Credentials [T1552] – The attacker may retrieve stored credentials from exposed logs.

Execution
- User Execution [T1204] – The attacker may trick an administrator into executing a malicious script via cross-site scripting.

Privilege Escalation
- Abuse Elevation Control Mechanism [T1548] – Exploiting broken access control to perform unauthorized admin-level actions.

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

Attackers typically target industries that rely heavily on VMware Aria Operations and Aria Operations for Logs to manage virtualized environments, cloud workloads, and large-scale IT infrastructure. Many industries are at risk:

- Finance
- Education
- Manufacturing
- Government
- Small to Medium Sized Businesses (SMBs)
- Transportation
- Retail
- Telecommunications
- Energy
- 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

Support Content Notification - Support Portal - Broadcom support portal