مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of VMware Aria Operations & VMware Tools Vulnerabilities

Tracking #:432317763

Date:30-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Broadcom has released security updates addressing an actively exploited zero-day vulnerability in VMware Aria Operations and VMware Tools.

TECHNICAL DETAILS:

Broadcom has released security updates addressing an actively exploited zero-day vulnerability in VMware Aria Operations and VMware Tools.

A local privilege escalation (LPE) vulnerability, tracked as CVE-2025-41244, is now confirmed to be under active exploitation in the wild by the UNC5174 threat group.

The flaw affects both VMware Tools and the Service Discovery Management Pack (SDMP) within VMware Aria Operations, allowing unprivileged local users to escalate privileges to root without authentication.

Since October 2024, UNC5174 has been observed weaponizing this vulnerability to gain persistence and expand control within hybrid-cloud environments, significantly raising the likelihood of advanced persistent threats (APTs) targeting enterprises using VMware hypervisors. Two additional vulnerabilities (CVE-2025-41245 – Information Disclosure, and CVE-2025-41246 – Improper Authorization in VMware Tools) further increase risk exposure.

Vulnerability Details

1. **CVE-2025-41244 – Local Privilege Escalation**
   - CVSS 3.1 Score: 7.8 (High)
   - Affected Components: VMware Tools (open-vm-tools), Aria Operations SDMP
   - Impact: Unprivileged users can escalate to root on the same VM.
   - Exploitation: Active exploitation in the wild by UNC5174.
   - Root Cause:
     - Credential-based mode: Vulnerability in Aria Operations metrics-collector scripts.
     - Credential-less mode: Flaw in get-versions.sh script of open-vm-tools due to overly broad regex patterns.

2. **CVE-2025-41245 – Information Disclosure**
   - CVSS 3.1 Score: 4.9 (Moderate)
   - Affected Component: VMware Aria Operations
   - Impact: Non-admin users may disclose credentials of other Aria Operations users.
   - Exploitation: Not yet observed in the wild.

3. **CVE-2025-41246 – Improper Authorization**
   - CVSS 3.1 Score: 7.6 (High)
   - Affected Component: VMware Tools (Windows only)
   - Impact: Non-admin VM users authenticated via vCenter/ESX may access other guest VMs with valid credentials.
   - Exploitation: Not yet confirmed.
   - Note: Linux and macOS builds of VMware Tools are unaffected.

Impacted Products

- VMware Aria Operations (8.x, 5.x, 4.x, 3.x, 2.x)
- VMware Tools (Windows, Linux) – versions 11.x, 12.x, 13.x
- VMware Cloud Foundation (including Operations)
- VMware Telco Cloud Platform
- VMware Telco Cloud Infrastructure

RECOMMENDATIONS:

- Patch Immediately – Apply vendor-provided patches and KB updates as per the response matrix.
- Process Monitoring-Alert on child processes spawned by vmtoolsd or Aria SDMP that originate from non-standard paths.
- Monitor suspicious execution of get-versions.sh or custom scripts leveraging SDMP.
- Limit guest VM access to internal/management networks
- Enforce least privilege for all VM and Aria Operations accounts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERNCES:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149