Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

VMware Aria and Tools Vulnerabilities Fixed Amid Ongoing Exploitation

Date of Publication	Admiralty Code	TA Number
October 1, 2025	A1	TA2025302

Summary

Discovered On: Mid-October 2024
Affected Products: VMware Aria Operations, VMware Tools, VMware Cloud Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure
Actor: UNC5174 (aka Uteus)
Impact: Broadcom has rolled out critical fixes for multiple VMware vulnerabilities, one of which (CVE-2025-41244) is already being exploited in the wild by UNC5174 to escalate privileges from a regular user to full root access on guest VMs. Alongside this zero-day, other flaws addressed are CVE-2025-41245 and CVE-2025-41246 that could let attackers move laterally across VMs if they hold valid credentials. With proof-of-concept exploits circulating and active attacks confirmed, organizations are urged to patch immediately, lock down local access, and tighten controls on vCenter and ESX accounts to prevent attackers from turning a single foothold into a full environment compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-41244	VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability	VMware Aria Operations and VMware Tools	✓	✗	✓
CVE-2025-41245	VMware Aria Operations Information Disclosure Vulnerability	VMware Aria Operations	✗	✗	✓
CVE-2025-41246	VMware Tools Improper Authorisation Vulnerability	VMware Tools for Windows	✗	✗	✓

Vulnerability Details

#1

Broadcom has released patches for multiple vulnerabilities in VMware Aria Operations and VMware Tools, tracked as CVE-2025-41244, CVE-2025-41245, and CVE-2025-41246. These flaws vary in impact, but together they create serious risks to confidentiality and host integrity. Notably, CVE-2025-41244 has been weaponized in real-world attacks since mid-October 2024, raising the urgency for administrators to apply fixes without delay.

#2

CVE-2025-41244 is a local privilege-escalation bug that lets a non-privileged user on a guest VM raise their privileges to root when VMware Tools is installed and the VM is managed by Aria Operations with SDMP enabled. In short: an attacker with only local access to a VM can leverage the service discovery and VMware tooling to obtain full control of that VM if the environment matches the vulnerable configuration.

#3

CVE-2025-41245 and CVE-2025-41246 target different aspects of the stack. The former is an information-disclosure issue in Aria Operations that can allow a low-privilege user to expose other users' credentials. The latter is an improper-authorization defect in VMware Tools for Windows that in constrained scenarios where an attacker already has valid credentials and vCenter/ESX authentication, could be abused to access other guest VMs. Successful exploitation of CVE-2025-41246 requires knowledge of the target VM credentials and an authenticated session with vCenter or ESX.

#4

Public proof-of-concept activity for CVE-2025-41244 shows attackers staging malicious binaries in commonly writable locations (examples observed in the wild include paths like /tmp/httpd) and ensuring those binaries appear in the guest process tree and open a listening socket so VMware's discovery picks them up. Because of confirmed zero-day exploitation (attributed to UNC5174), organizations should urgently upgrade to the fixed Broadcom releases for VMware Tools and VMware Aria Operations. As immediate hardening steps, restrict untrusted local access to VMs, monitor for unfamiliar binaries and listening sockets in guest processes, and review Aria Operations user privileges while you deploy the patches.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-41244	VMware Cloud Foundation and VMware vSphere Foundation: VMware Cloud Foundation Operations Version Prior to 9.0.1.0, VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 3.0.5.0, Prior to 13.0.5, Prior to 12.5.4, VMware Cloud Foundation: VMware Aria Operations Version 5.x, 4.x, VMware Aria Operations Version Prior to 8.18.5	cpe:2.3:a:vmware:vmware_cloud_foundation_operations:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_tools:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:*:*	CWE-267
CVE-2025-41245	VMware Aria Operations Version Prior to 8.18.5, VMware Cloud Foundation: VMware Aria Operations Version 5.x, 4.x,	cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:*:*	CWE-1188
CVE-2025-41246	VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 13.0.5.0, Prior to 12.5.4	cpe:2.3:a:vmware:vmware_tools:*:*:*:*:*:*:*:*:*	CWE-863

Recommendations

Patch Immediately: Install the latest updates for VMware Aria Operations and VMware Tools released by Broadcom. This is the most effective way to close the vulnerabilities, especially CVE-2025-41244, which attackers are already exploiting.

Limit Local Access: Reduce the number of users who have local, non-administrative accounts on guest VMs. The fewer people who can log in, the harder it is for attackers to take advantage of these flaws.

Monitor Unusual Activity: Keep an eye on your VMs for suspicious binaries, especially in common writable paths like /tmp/. Look for unknown processes opening listening sockets, which may indicate exploitation attempts.

Review User Permissions: Double-check Aria Operations accounts and remove unnecessary privileges. This reduces the impact of the information-disclosure flaw (CVE-2025-41245).

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1036** Masquerading	**T1036.005** Match Legitimate Resource Name or Location
T1068 Exploitation for Privilege Escalation	**T1552** Unsecured Credentials		

Patch Link

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

References

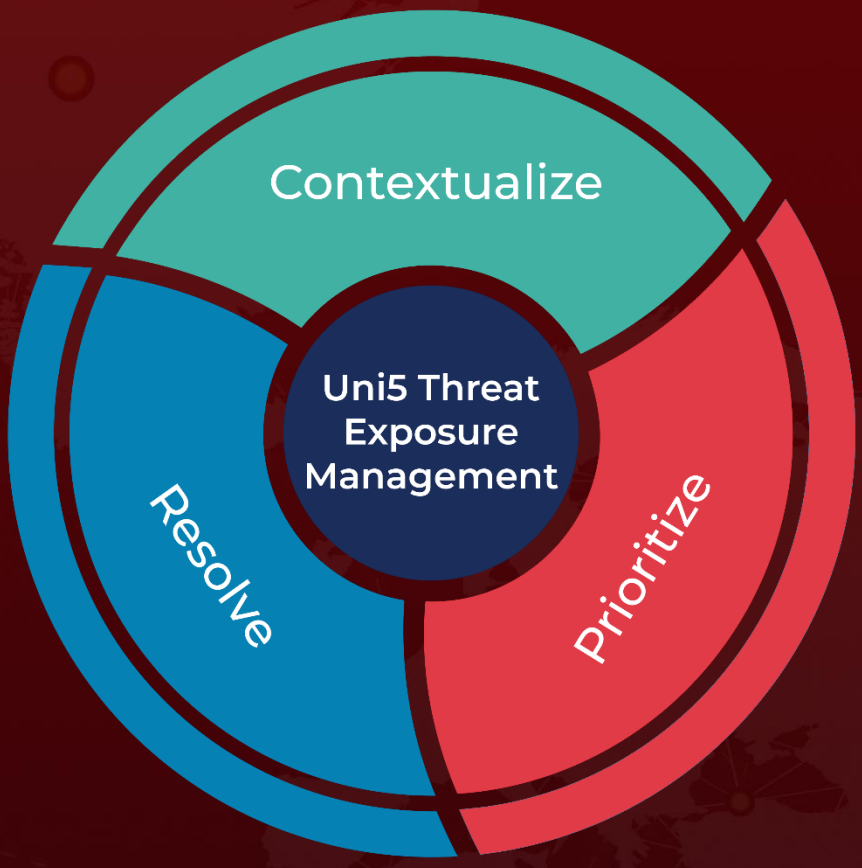
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 1, 2025 . 7:30 AM

More at www.hivepro.com