Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

VMware Patches Aria Operations Flaws as Exploitation Emerges in the Wild

Date of Publication	Admiralty Code	TA Number
March 05, 2026	A1	TA2026061

Summary

First Seen: February 24, 2026
Affected Products: VMware Aria Operations, VMware Cloud Foundation, VMware vSphere Foundation, VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure
Impact: VMware has released urgent security updates to address multiple vulnerabilities affecting VMware Aria Operations, including the actively exploited flaw CVE-2026-22719. The vulnerability allows attackers to execute arbitrary operating system commands without authentication during support-assisted migration workflows, potentially giving them full control of affected appliances. Alongside this flaw, VMware also patched a stored cross-site scripting vulnerability (CVE-2026-22720) and a privilege escalation issue (CVE-2026-22721), both of which could enable attackers with limited access to compromise administrative accounts. Organizations using affected versions are strongly urged to apply the latest patches or available mitigations immediately to reduce the risk of system compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-22719	Broadcom VMware Aria Operations Command Injection Vulnerability	Broadcom VMware Aria Operations	✗	✓	✓
CVE-2026-22720	VMware Aria Operations Stored Cross-Site Scripting Vulnerability	Broadcom VMware Aria Operations	✗	✗	✓
CVE-2026-22721	VMware Aria Operations Privilege Escalation Vulnerability	Broadcom VMware Aria Operations	✗	✗	✓

Vulnerability Details

#1 VMware has released security updates addressing several vulnerabilities in its products, including a flaw tracked as CVE-2026-22719. This vulnerability stems from insufficient input validation within a component used during support-assisted product migration workflows in VMware Aria Operations. An attacker can exploit this weakness to inject and execute arbitrary operating system commands on the underlying Aria Operations appliance. The severity of the issue is underscored by its exploitation in real-world attacks.

#2 The vulnerability impacts multiple versions of Aria Operations, including releases 8.x through 8.18.5 and 9.x through 9.0.1. It also affects environments where the platform is deployed as part of broader VMware solutions such as VMware Cloud Foundation (versions 4.x, 5.x, and 9.x), VMware Telco Cloud Platform (versions 4.x and 5.x), and VMware Telco Cloud Infrastructure (versions 2.x and 3.x). To mitigate the risk, Broadcom, which now maintains VMware products, has released a workaround shell script documented in KB430349 that specifically addresses this vulnerability.

#3 Another issue resolved in the same advisory is CVE-2026-22720, a stored cross-site scripting (XSS) flaw affecting the custom benchmark creation feature in VMware Aria Operations. The vulnerability occurs because user-supplied input is not adequately sanitized before being stored and later rendered in the web management interface. A threat actor with sufficient privileges to create custom benchmarks can inject persistent JavaScript code, which will execute in the browser of any administrator who views the affected benchmark entry. This flaw impacts the same product versions as CVE-2026-22719 and has been fixed in Aria Operations 8.18.6 and Cloud Foundation Operations 9.0.2.0.

#4 The third vulnerability, CVE-2026-22721, allows attackers to escalate privileges within the Aria Operations environment. An attacker who already possesses sufficient permissions in VMware vCenter to access Aria Operations can exploit this flaw to gain full administrative control over the platform. This is particularly concerning in enterprise environments that rely on privilege separation between vCenter and Aria Operations for defense-in-depth.

#5 Broadcom has acknowledged reports suggesting that CVE-2026-22719 already been exploited in the wild. Administrators are therefore strongly advised to apply the latest security updates for VMware Aria Operations or deploy the recommended workaround immediately to reduce exposure, particularly in environments where migration workflows are active. Prompt remediation is critical to prevent potential remote compromise of affected systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-22719	Broadcom VMware Cloud Foundation, Broadcom VMware vSphere Foundation Version Before 9.0.2.0 Broadcom VMware Aria Operations (Before 8.18.6 / Before 9.0.2.0), VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure	cpe:2.3:a:vmware:aria_operations:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*	CWE-77
CVE-2026-22720			CWE-79
CVE-2026-22721			CWE-269

Recommendations

Apply Vendor Patches Immediately: Upgrade VMware Aria Operations to version 8.18.6 or VMware Cloud Foundation Operations to version 9.0.2.0 without delay. These patched releases address all three disclosed vulnerabilities (CVE-2026-22719, CVE-2026-22720, and CVE-2026-22721). Given that CVE-2026-22719 has been confirmed as actively exploited, patching should be treated as the highest priority remediation action for all affected deployments.

Deploy the Workaround Script for CVE-2026-22719. If Immediate Patching Is Not Feasible: If operational constraints prevent immediate patching, apply Broadcom's workaround shell script (aria-ops-rce-workaround.sh) as documented in KB430349 to mitigate the command injection vulnerability. Note that this workaround addresses only CVE-2026-22719 and does not protect against CVE-2026-22720 or CVE-2026-22721, so it should be considered a temporary measure until full patching is complete.

Restrict Network Access to the Aria Operations Management Interface: Limit network-level access to the VMware Aria Operations management interface to only authorized administrative hosts and networks. Apply firewall rules, network segmentation, and access control lists to prevent unauthorized network entities from reaching the management plane, thereby reducing the attack surface for all three vulnerabilities, particularly the unauthenticated command injection in CVE-2026-22719.

Audit Custom Benchmarks and User Privileges: Review all existing custom benchmarks within VMware Aria Operations for any indicators of injected malicious scripts, and audit user accounts with permissions to create or modify benchmarks. Remove or remediate any suspicious benchmark entries and ensure the principle of least privilege is enforced for all Aria Operations user roles to mitigate the stored XSS risk associated with CVE-2026-22720.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

References

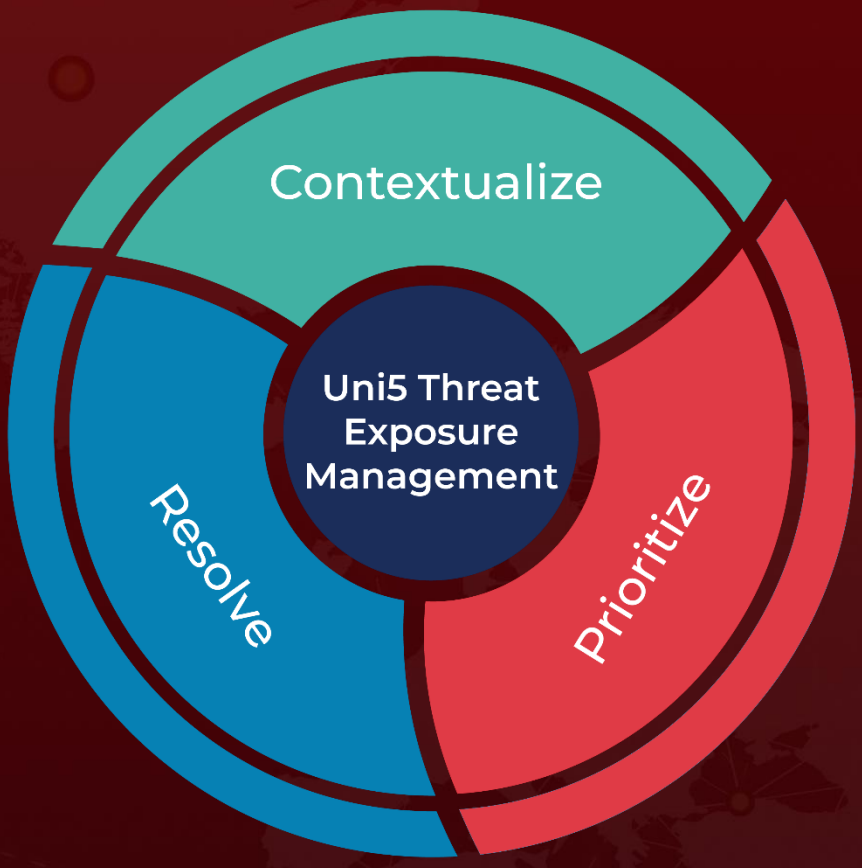
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

https://socradar.io/blog/cve-2026-22719-vmware-aria-operations/

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

March 05, 2026 • 6:00 AM

More at www.hivepro.com