AL2026_03 CISA Flags VMware Aria Operations RCE Flaw as Exploited in Attacks (March 6th, 2026)

Description

The Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability affecting VMware Aria Operations to its Known Exploited Vulnerabilities (KEV) catalog after confirming it is being actively exploited in cyberattacks.

The vulnerability, tracked as **CVE-2026-22719**, is a command injection flaw that could allow unauthenticated attackers to execute arbitrary commands on affected systems, potentially leading to remote code execution (RCE).

Successful exploitation may enable threat actors to gain control of affected environments, manipulate monitoring systems, or pivot deeper into enterprise infrastructure. Organizations using VMware Aria Operations are urged to patch affected systems immediately and follow vendor mitigation guidance.

Attack Details

The vulnerability impacts VMware Aria Operations environments and can be exploited under specific operational conditions.

Key details include:

- **Vulnerability:** CVE-2026-22719 – Command Injection leading to potential Remote Code Execution.
- **Exploitation status:** CISA has added the flaw to its KEV catalog, confirming it is actively exploited in the wild.
- **Attack vector:** An unauthenticated attacker may exploit the vulnerability to execute arbitrary commands on vulnerable systems during certain processes such as support-assisted product migration.
- **Potential impact:**
    - Unauthorized command execution on affected VMware systems.
    - Compromise of virtualization infrastructure and associated workloads.
    - Ability for attackers to pivot into broader enterprise networks or cloud resources managed by the platform.

Virtualization management platforms such as VMware Aria Operations often have visibility and control across large infrastructure environments, meaning compromise could provide attackers with significant operational access.

Remediation

Organizations running VMware Aria Operations should take the following mitigation actions immediately:

- **Apply vendor patches:** Install the latest security updates released by Broadcom to address CVE-2026-22719.
- **Review CISA KEV guidance:** Follow mitigation and remediation recommendations from the Cybersecurity and Infrastructure Security Agency for vulnerabilities listed in the KEV catalog.
- **Restrict network exposure:** Limit external access to VMware management interfaces and ensure they are not directly exposed to the internet where possible.
- **Monitor system logs:** Review logs for suspicious command execution, unusual administrative activity, or unauthorized access attempts.
- **Implement segmentation:** Isolate virtualization management infrastructure from general enterprise networks to reduce lateral movement risk.
- **Conduct vulnerability scanning:** Regularly scan infrastructure for outdated VMware components and ensure timely patching of virtualization platforms.
- **Enable strong authentication:** Enforce multi-factor authentication (MFA) for administrative access to virtualization management platforms.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Abrams, L. (2026). CISA flags VMware Aria Operations RCE flaw as exploited in attacks. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/cisa-flags-vmware-aria-operations-rce-flaw-as-exploited-in-attacks/