CYBER ADVISORY

TLP:CLEAR

16 January 2024

VMware Aria Automation Vulnerability

CVE-2023-34063 | RCE | Aria Automation | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-34063.[1] The vulnerability affects Aria Automation (formerly vRealize Automation) prior to version 8.16, as well as Cloud Foundation.[2] Exploitation of the vulnerability could allow an authenticated attacker to gain unauthorized access to remote organizations and workflows.[3,4]

Affected Product	Version	Fixed Version
VMware Aria Automation	8.14.x	8.14.1 + Patch
VMware Aria Automation	8.13.x	8.13.1 + Patch
VMware Aria Automation	8.12.x	8.12.2 + Patch
VMware Aria Automation	8.11.x	8.11.2 + Patch
VMware Cloud Foundation (Aria Automation)	5.x, 4.x	KB96136

Table 1: Vulnerable VMware versions and fixed versions

The Cal-CSIC recommends immediately applying the appropriated upgrade of the affected VMWare product.

For further information on applying upgrades, please refer to VMware Security Advisories.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Affairs; "Vmware Fixed A Critical Flaw In Aria Automation. Patch It Now!;" https://securityaffairs.com/157576/security/vmware-aria-automation.html; accessed 16 January 2024

[2] Sec Alerts; "CVE-2023-34063;" https://secalerts.co/vulnerability/CVE-2023-34063; accessed 16 January 2024

[3] National Vulnerability Database; "CVE-2023-34063 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2023-34063; accessed 16 January 2024

[4] Security Week; "VMware Urges Customers to Patch Critical Aria Automation Vulnerability;" https://www.securityweek.com/vmware-urges-customers-to-patch-critical-aria-automation-vulnerability/; accessed 16 January 2024