

VMware Patches Pre-Auth Code Execution Flaw in Logging Product

Virtualization technology powerhouse VMware continues to encounter major security problems in its enterprise-facing log analysis product.

The company shipped urgent patches on Thursday to cover critical security defects in the VMware Aria Operations for Logs (formerly vRealize Log Insight) product line and warned of the risk of pre-authentication remote root exploits.

A critical-level advisory from VMware documents two separate vulnerabilities – CVE-2023-20864 and CVE-2023-20865 – in the VMware Aria Operations for Logs suite and provides guidance to help businesses mitigate the issues.

“An unauthenticated, malicious actor with network access to VMware Aria Operations for Logs may be able to execute arbitrary code as root,” the company said in its documentation of the CVE-2023-20864 vulnerability. The flaw carries a CVSS severity score of 9.8 out of 10.

The second vulnerability is described as a command injection issue with a CVSS score of 7.2/10.

“A malicious actor with administrative privileges in VMware Aria Operations for Logs can execute arbitrary commands as root,” according to the advisory.

VMware’s security troubles with the vRealize Logging product line are well known. The company has patched several high-severity issues in the past and confirmed the release of

exploit code targeting known software bugs.

The VMWare vRealize product has been featured in the CISA KEV (Known Exploited Vulnerabilities) must-patch catalog.

Related: VMware Patches VM Escape Flaw Exploited at Geekpwn Event

Related: VMware Confirms Exploit Code Released for Critical vRealize Logging Flaws

Related: VMware Patches High-Severity Vulnerabilities in vRealize Operations

VMware Patches Pre-Auth Code Execution Flaw in Logging Product