Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Attackers Exploit VMware's Aria Operations for Logs Vulnerability

Date of Publication	Admiralty Code	TA Number
October 25, 2023	A1	TA2023433

Summary

First Seen: October 19, 2023
Affected Platform: VMware Aria Operations for Logs
Impact: A critical authentication bypass vulnerability (CVE-2023-34051) in VMware Aria Operations for Logs allows remote code execution with root privileges under certain conditions, raising concerns for compromised networks. The security patch attempted to address the issue by blocking Thrift ports but left other vulnerabilities unpatched, which attackers can bypass by spoofing their IP address.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-34051	VMware Aria Operations for Logs Authentication Bypass Vulnerability	VMware Aria Operations for Logs	☒	☒	✓
CVE-2023-34052	VMware Aria Operations for Logs Deserialization Vulnerability	VMware Aria Operations for Logs	☒	☒	✓

Vulnerability Details

#1

VMware has alerted its customers about the availability of proof-of-concept (PoC) exploit code for a critical authentication bypass vulnerability (CVE-2023-34051) in vRealize Log Insight, now known as VMware Aria Operations for Logs, along with CVE-2023-34052.

#2

This flaw allows unauthenticated attackers to remotely execute code with root privileges under certain conditions. The successful exploitation relies on the attacker compromising a host within the target environment and having permissions to add an extra interface or static IP address.

#3

These vulnerabilities serve as a bypass for a chain of critical flaws (CVE-2022-31706, CVE-2022-31707, CVE-2022-31711) patched by VMware in January, which were chained together and exploited by attackers to gain remote code execution. VMware had earlier provided patches for these vulnerabilities; however, the patches are now found to be incomplete. The patch rationale was that vulnerabilities exploitation required access to the Thrift ports, blocking access to these ports should mitigate the risks.

#4

Attackers could bypass the patch by spoofing their IP address, thereby gaining access to the exposed Thrift ports and exploiting the other vulnerabilities. The attack relies on having at least two VMware Aria Operations for Logs instances in a master/worker configuration, and an attacker machine with the same source IP address as the worker node. While the attack requires some infrastructure setup, it's a significant concern, especially in compromised networks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34051	Vmware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12	cpe:2.3:a:vmware:vreaalize_log_insight:8.12:*:*:*:*:*:*:*	CWE-287
CVE-2023-34052	Vmware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12	cpe:2.3:a:vmware:vreaalize_log_insight:8.12:*:*:*:*:*:*:*	CWE-502

Recommendations

Patch and Update Immediately: Ensure that your VMware Aria Operations for Logs (formerly vRealize Log Insight) is updated with the latest patches and security updates to address the authentication bypass vulnerability (CVE-2023-34051) and other related vulnerabilities, such as CVE-2023-34052. Stay proactive in keeping your systems up-to-date.

Defense in Depth: Relying solely on official patches is not enough. Implement a defense-in-depth strategy, which includes multiple layers of security measures. This can help protect your environment from potential bypasses and exploits.

Vulnerability Scanning and Assessment: Conduct regular vulnerability scans and assessments of your IT infrastructure. Identify and address any vulnerabilities promptly to reduce the attack surface.

Implement continuous monitoring: Monitor the network, endpoints, and logs for Indicators of Compromise (IoCs). This helps in detecting and responding to any potential security incidents.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0005 Defense Evasion	TA0002 Execution
TA0040 Impact	T1588.006 Vulnerabilities	T1588.005 Exploits	T1588 Obtain Capabilities
T1036 Masquerading	T1068 Exploitation for Privilege Escalation	T1071 Application Layer Protocol	T1203 Exploitation for Client Execution

Patch Details

https://www.vmware.com/security/advisories/VMSA-2023-0021.html

References

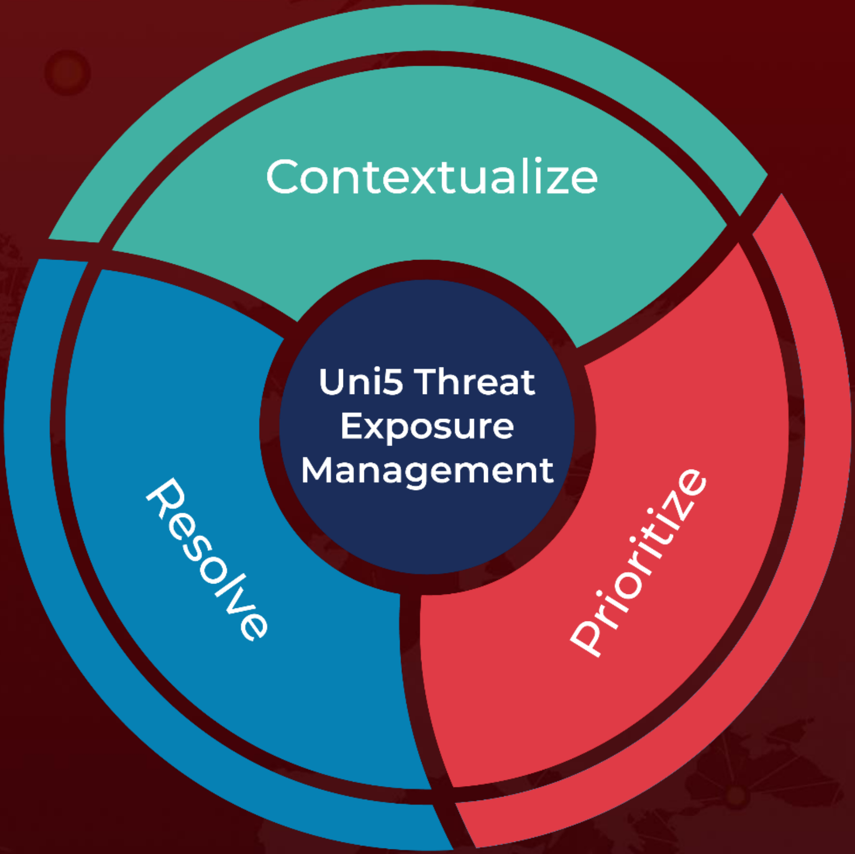
https://www.horizon3.ai/vmware-aria-operations-for-logs-cve-2023-34051-technical-deep-dive-and-iocs/

https://www.hivepro.com/vmware-addresses-security-flaws-in-vrealize-log-insight/

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 25, 2023 • 6:30 AM

More at www.hivepro.com