Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Exploit found in the wild for Critical VMware Aria Operations Bug

Date of Publication	Admiralty Code	TA Number
July 12 , 2023	A1	TA2023295

Summary

First Seen: April 20, 2023
Affected Product: VMware Aria Operations for Logs
Impact: An exploit has surfaced for CVE-2023-20864, a highly significant security vulnerability within the VMware Aria Operations for Logs analysis tool utilized in cloud management. This exploit empowers malicious actors to execute arbitrary code with root privileges, without requiring any user interaction.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-20864	VMware Aria Operations for Logs Deserialization Vulnerability	Aria Operations for Logs: before 8.12	✗	✗	✓
CVE-2023-20865	VMware Aria Operations for Logs Command Injection Vulnerability	Aria Operations for Logs: before 8.12	✗	✗	✓

Vulnerability Details

#1

VMware has issued a warning, informing that exploit code has become available for a critical vulnerability, CVE-2023-20864, in the VMware Aria Operations for Logs analysis tool. This tool facilitates administrators in efficiently managing large volumes of application and infrastructure logs within extensive operational environments.

#2

CVE-2023-20864 represents a deserialization vulnerability within VMware Aria Operations for Logs (formerly vRealize Log Insight). A remote attacker, without proper authentication, who has the ability to access VMware Aria Operations for Logs, could potentially exploit this vulnerability to gain arbitrary code execution with the highest system privileges.

#3

On the other hand, CVE-2023-20865 denotes an operating system (OS) command injection vulnerability discovered in VMware Aria Operations for Logs. In this scenario, an attacker with authenticated access to a vulnerable instance of VMware Aria Operations for Logs and administrative privileges could exploit this vulnerability to achieve arbitrary code execution with root-level privileges. Additionally, VMware has recently issued an alert regarding a critical bug (CVE-2023-20887) in VMware Aria Operations for Networks, which has since been patched. This vulnerability allows for remote command execution with root-level privileges.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20864	Aria Operations for Logs version: 8.10.2 and 4.x	cpe:2.3:a:vmware:vreaalize_log_insight:*:*:*:*:*:*:*:*	CWE-502
CVE-2023-20865	Aria Operations for Logs: version 8.10.2, 8.10, 8.8.x, 8.6.x		CWE-77

Recommendations

Administrators should give high priority to promptly applying patches for CVE-2023-20864 as a precautionary measure against potential attacks, considering that VMware has confirmed the availability of exploit code in the wild. Ensuring that VMware vRealize instances are kept up to date with the latest **patches** not only mitigates the risk of exploitation but also enhances the overall security posture of the system

While the number of online-exposed VMware vRealize instances is relatively low, it's crucial to reinforce network segmentation practices. By restricting external access and limiting the exposure of these instances to internal networks only, organizations can reduce the attack surface and mitigate potential risks.

Establish comprehensive monitoring systems to detect any unusual or suspicious activities within the VMware Aria Operations for Logs environment. Employ intrusion detection and prevention systems (IDPS) along with log analysis tools to proactively identify signs of potential exploitation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0040 Impact	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation

Patch Details

Update to VMware Aria Operations for Log version 8.12

Patch Link:
https://www.vmware.com/security/advisories/VMSA-2023-0007.html

References

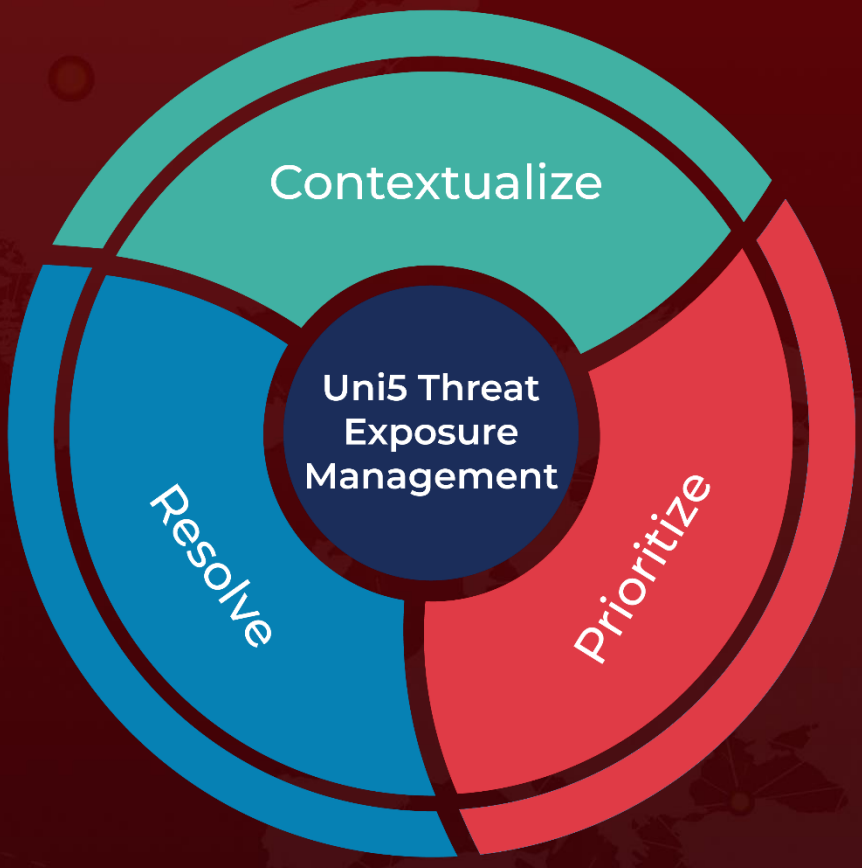
https://www.darkreading.com/cloud/critical-vmware-bug-exploit-code-released

https://www.hivepro.com/critical-vulnerabilities-in-vmware-aria-operations-addressed-and-secured/

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

July 12 2023 . 6:00 AM

More at www.hivepro.com