

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Vulnerabilities in VMware Aria Operations Addressed and Secured

Date of Publication

June 08, 2023

Admiralty Code

A1

TA Number

TA2023255










Summary

First Seen: June 7, 2023

Affected Platforms: VMware Aria Operations Networks

Impact: These three vulnerabilities could allow attackers to remotely execute code, access sensitive information, and potentially disrupt network operations, posing significant risks to organizations.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-20887	VMWare Aria Operations for Networks Command Injection Vulnerability	VMware Aria Operations Networks			
CVE-2023-20888	VMWare Aria Operations for Networks Authenticated Deserialization Vulnerability	VMware Aria Operations Networks			
CVE-2023-20889	VMWare Aria Operations for Networks Information Disclosure Vulnerability	VMware Aria Operations Networks			

Vulnerability Details

#1

VMware has released several security patches to address critical and high-severity vulnerabilities in VMware Aria Operations for Networks. These vulnerabilities could allow attackers to gain remote execution capabilities or access sensitive information. The most severe vulnerability, CVE-2023-20887, enables unauthenticated threat actors to perform command injection attacks, resulting in remote code execution.

#2

Another vulnerability, CVE-2023-20888, requires authenticated access and can lead to remote code execution through a deserialization weakness. The third flaw, CVE-2023-20889, allows information disclosure after a successful command injection attack. There are no workarounds available, so administrators must patch all vulnerable installations.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20887	VMWare Aria Operations for Networks (formerly vRealize Network Insight): 6.0.0 - 6.8.0	cpe:2.3:a:vmware:vrealize_network_insight:6.8.0:*:*:*:*:*:*	CWE-78
CVE-2023-20888			CWE-502
CVE-2023-20889			CWE-200

Recommendations



Apply Security Patches: Immediately install the security patches released by VMware to address the critical and high-severity vulnerabilities in VMware Aria Operations for Networks. Keep your software up to date by regularly checking for and applying the latest security updates and patches provided by the vendor.



Restrict Network Access: Implement strict network access controls to minimize the exposure of vulnerable systems. Use firewalls and network security devices to restrict access to trusted sources only. Properly segment your network and apply access controls to limit the network access to the vulnerable appliance.



Enforce Strong Authentication: Implement strong authentication mechanisms such as complex and unique passwords or multi-factor authentication (MFA) to secure access to VMware Aria Operations for Networks. Ensure that users and administrators follow secure password practices and enforce regular password changes to prevent unauthorized access.



Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0007 Discovery	TA0002 Execution	TA0040 Impact
TA0003 Persistence	TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation	T1012 Query Registry
T1059 Command and Scripting Interpreter	T1082 System Information Discovery	T1055 Process Injection	T1018 Remote System Discovery
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1203 Exploitation for Client Execution

Patch Details

<https://kb.vmware.com/s/article/92684>

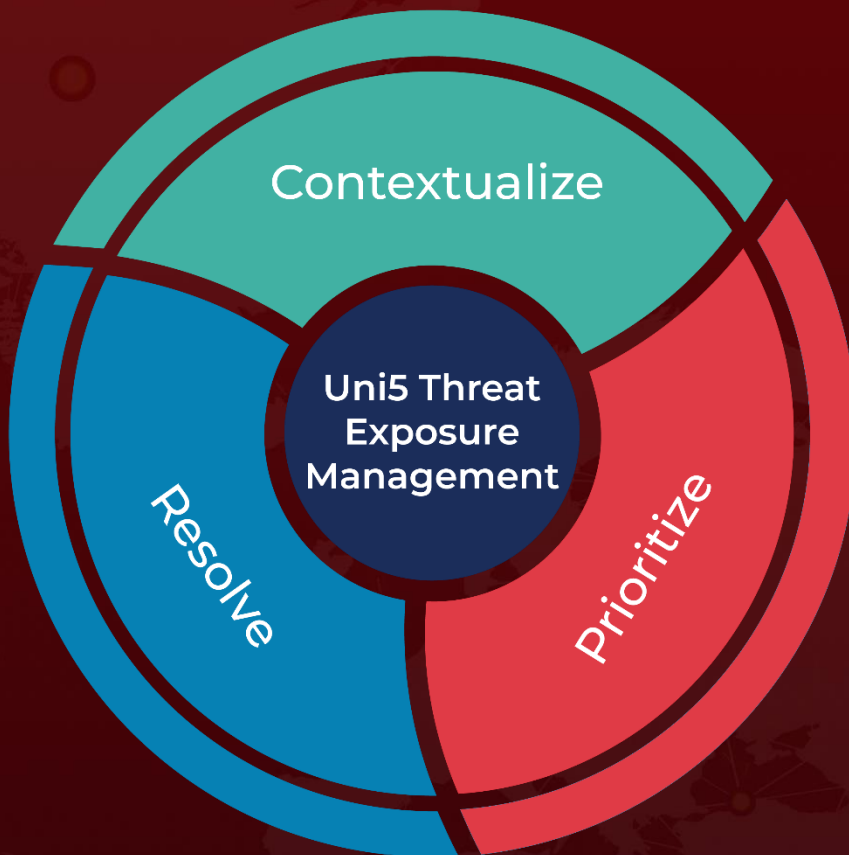
References

<https://www.vmware.com/security/advisories/VMSA-2023-0012.html>

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

June 08, 2023 • 5:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com