Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Critical Vulnerability uncovered in VMware Aria Operations for Networks

Date of Publication	Admiralty Code	TA Number
August 31, 2023	A1	TA2023351

Summary

First Seen: August 29, 2023
Affected Products: VMware Aria Operations for Networks
Impact: Two vulnerabilities have been discovered in VMware Aria Operations for Networks (formerly vRealize Network Insight). The first vulnerability, CVE-2023-34039, is an authentication bypass that allows attackers to access the network CLI. The other vulnerability, CVE-2023-20890, enables remote code execution through arbitrary file write.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-34039	VMware Aria Operations for Networks Authentication Bypass Vulnerability	VMware Aria Operations for Networks	☒	☒	✓
CVE-2023-20890	VMware Aria Operations for Networks Arbitrary File Write Vulnerability	VMware Aria Operations for Networks	☒	☒	✓

Vulnerability Details

#1 Two recently discovered vulnerabilities, namely CVE-2023-34039 and CVE-2023-20890, have emerged within Aria Operations for Networks. The critical issues associated with CVE-2023-34039 stem from instances of authentication bypass due to inadequate generation of unique cryptographic keys. The second flaw, CVE-2023-20890, constitutes an arbitrary file write vulnerability, leveraging administrative privileges to inscribe files in unrestricted destinations, ultimately enabling the remote code execution.

#2 The CVE-2023-34039 vulnerability allows a malicious actor to illicitly enter Aria Operations for Networks and circumvent SSH authentication, thereby obtaining unauthorized access to the Aria Operations for Networks CLI.

#3 Multiple versions of Aria Operations Networks have been impacted by these vulnerabilities. Both the vulnerabilities are fixed in version 6.11, VMware have also released the patches for affected versions.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34039	VMware Aria Operations for Networks Versions 6.2 ,6.3 , 6.4 , 6.5.1 , 6.6 , 6.7 , 6.8 , 6.9 , 6.10	cpe:2.3:a:vmware:aria_operations_for_networks:*:*:*:*:*:*:*:*	CWE-327
CVE-2023-20890	VMware Aria Operations for Networks Versions 6.2 ,6.3 , 6.4 , 6.5.1 , 6.6 , 6.7 , 6.8 , 6.9 , 6.10	cpe:2.3:a:vmware:aria_operations_for_networks:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Apply Patch and Update the Software: Install the security patches provided by VMware to address the CVE-2023-34039 & CVE-2023-20890.

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Monitoring and Logging: Set up monitoring and logging mechanisms to track authentication events. Monitor for any unusual activity and promptly investigate and respond to suspicious behavior.

Limit service exposure: Ensure that VMware Aria Operations for Networks services are only exposed to a restricted network area.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0004** Privilege Escalation	**TA0006** Credential Access	**TA0003** Persistence
TA0011 Command and Control	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	**T1059.008** Network Device CLI
T1105 Ingress Tool Transfer	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1588.006** Vulnerabilities

Patch Link

https://kb.vmware.com/s/article/94152

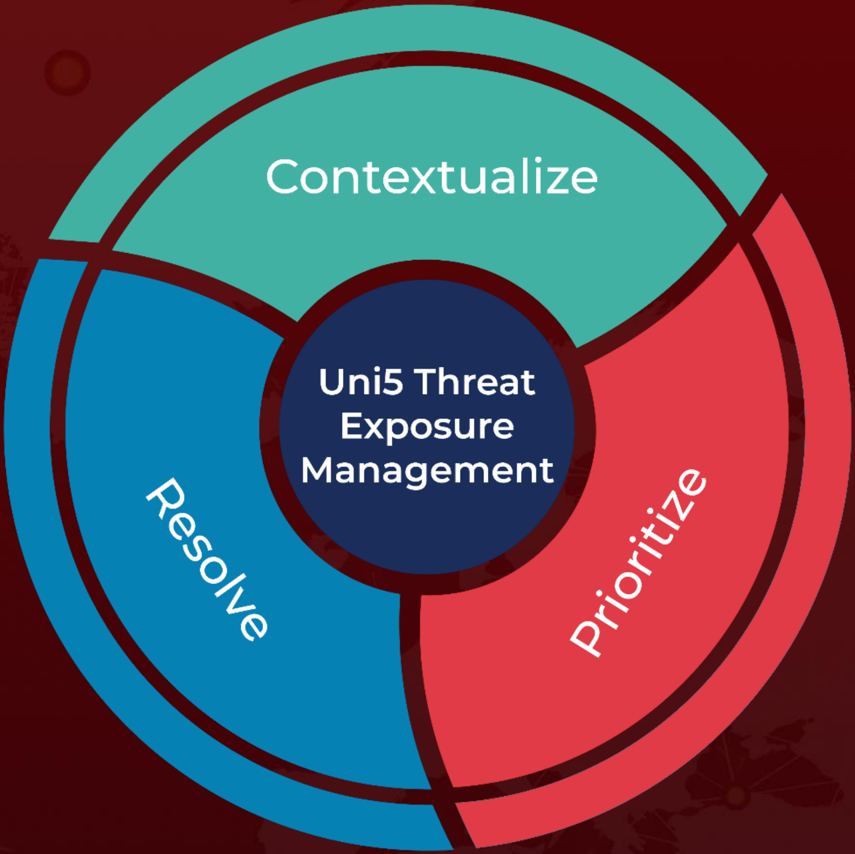
References

https://www.vmware.com/security/advisories/VMSA-2023-0018.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

August 31, 2023 • 7:30 AM

More at www.hivepro.com