Advisory Alert

Alert Number: **AAA20230830** **Date:** **August 30, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-34039, CVE-2023-20890)
Description	VMware has released security updates addressing Multiple vulnerabilities that exist in their VMware Aria products. **CVE-2023-34039 -** Aria Operations for Networks contains a critical Authentication Bypass vulnerability due to a lack of unique cryptographic key generation. This vulnerability allows a malicious actor with network access to bypass SSH authentication and gain unauthorized access to the Aria Operations for Networks CLI. **CVE-2023-20890 -** Aria Operations for Networks contains an important arbitrary file write vulnerability. An authenticated malicious actor with administrative access to VMware Aria Operations for Networks can write files to arbitrary locations, potentially leading to remote code execution. VMware recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	VMware Aria Operations Networks 6.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0018.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.