CERT-EU

Security Advisory 2023-060

Critical Vulnerability in VMware Aria Operations for Networks

August 31, 2023 — v1.0

TLP:CLEAR

History:

- *31/08/2023 — v1.0 – Initial publication*

Summary

On August 29, VMware released security updates to patch one critical (CVE-2023-34039) and one high-severity (CVE-2023-20890) vulnerability in Aria Operations for Networks, its enterprise network monitoring tool [1]. The flaws were responsibly reported to the vendor and as of the time of writing, there is no evidence of exploitation in the wild.

CERT-EU urges users to promptly apply the provided fixes [2].

Technical Details

Critical Vulnerability (CVE-2023-34039)

Aria Operations for Networks contains an Authentication Bypass vulnerability due to a lack of unique cryptographic key generation. This vulnerability may allow an attacker with network access to Aria Operations for Networks, to bypass SSH authentication and gain unauthorised access to the Aria Operations for Networks command-line interface (CLI).

High-Severity Vulnerability (CVE-2023-20898)

Aria Operations for Networks contains an arbitrary file write vulnerability. An authenticated malicious actor with administrative access to VMware Aria Operations for Networks could exploit this vulnerability to write files to arbitrary locations, potentially resulting in remote code execution.

Affected Products

The versions of the product starting with **6.2** and prior to **6.11** are impacted.

Recommendations

The vulnerabilities are fixed in versions **6.11** [2].

Workarounds

There is no workaround available for these vulnerabilities.

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0018.html

[2] https://kb.vmware.com/s/article/94152