Security Advisory 2023-081

Multiple Vulnerabilities in VMware Aria Operations for Logs

October 24, 2023 — v1.0

TLP:CLEAR

History:

- *24/10/2023 — v1.0 – Initial publication*

Summary

On 19 October 2023, VMware has released security updates to address two vulnerabilities affecting Aria Operations for Logs. The exploitation of the vulnerabilities could lead to Remote Code Execution and Authentication bypass. The vulnerabilities are tracked as `CVE-2023-34051` and `CVE-2023-34052` with a CVSS score of 8.1.[1]

It is recommended updating as soon as possible.

Technical Details

- **CVE-2023-34051**: This vulnerability (CVSS score of 8.1) allows an unauthenticated, malicious actor to inject files into the operating system of an impacted appliance which can result in remote code execution.
- **CVE-2023-34052**: This vulnerability (CVSS score of 8.1) allows a malicious actor with non-administrative access to the local system to trigger the deserialisation of data which could result in authentication bypass.

Affected Products

- VMware Aria Operations for Logs running on version 8.x before version 8.14;
- VMware Cloud Foundation (VMware Aria Operations for Logs) running on versions 5.x and 4.x.

Recommendations

CERT-EU recommends updating to the latest version as soon as possible.

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0021.html