CERT-EU

Security Advisory 2023-036

Critical Vulnerabilities in VMware Aria Operations for Networks

June 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/06/2023 — v1.0 – Initial publication*

Summary

On June 7, 2023, VMware issued multiple security patches to address critical vulnerabilities in VMware Aria Operations for Networks, formerly known as vRealize Network Insight. The vulnerabilities allow attackers to gain remote execution or access sensitive information [1].

CERT-EU recommends upgrading as soon as possible.

Technical Details

- **CVE-2023-20887**

This critical severity vulnerability, with a CVSS score of 9.8 out of 10, allows an unauthenticated attacker to perform a command injection attack resulting in remote code execution.

- **CVE-2023-20888**

This vulnerability, with a CVSS score of 9.1 out of 10, allows an authenticated attacker with a valid `member` role to perform a deserialisation attack resulting in remote code execution.

- **CVE-2023-20889**

This vulnerability, with a CVSS score of 8.8 out of 10, allows unauthenticated attacker to perform a command injection attack resulting in information disclosure.

Affected Products

VMware Aria Operations Networks version 6.x are affected by these vulnerabilities. The fixed version is KB92684 [1].

Recommendations

CERT-EU highly recommends updating the affected products to the fixed version.

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0012.html