U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0327

CISCO AND VMWARE PATCH CRITICAL FLAW

DATE ISSUED: 15th June 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

VMware releases security updates for Aria Operations for Networks, addressing critical flaws with potential information disclosure and Remote Code Execution (RCE). Cisco also issues critical security fixes for privilege escalation vulnerabilities in Expressway Series and Telepresence Video Communication Server (VCS).

BREAKDOWN

VMware patched three critical vulnerabilities in Aria Operations. VMware Aria Operations is a cloud-based platform that simplifies and automates business IT operations management. The most severe of the three vulnerabilities is a command injection vulnerability, identified as CVE-2023-20887 (CVSS score: 9.8). This vulnerability could enable an attacker who has network access to execute remote code. VMware has also addressed another deserialisation vulnerability, known as CVE-2023-20888, which has received a CVSS score of 9.1 out of 10. The VMware Aria Operations Networks version 6.x has been fixed in subsequent releases, namely versions 6.2, 6.3, 6.4, 6.5.1, 6.6, 6.7, 6.8, 6.9, and 6.10. There are two significant security vulnerabilities in Cisco products. The first flaw (CVE-2023-20105, CVSS score: 9.6) enables an attacker to change passwords for any user, including administrative users, and impersonate them. The second vulnerability (CVE-2023-20192, CVSS score: 8.4) could allow an attacker with authentication to execute commands and modify system configuration settings.

REMEDIATION STEPS

- VMware advises administrators to apply the necessary security patches to all VMware Aria Operations Networks 6.x on-prem installations.
- Install and regularly update your Next Generation Anti-Virus (NGAV) and anti-malware software that scans the computer files to identify and remove malware.
- Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Hacker News	https://thehackernews.com/2023/06/urgent-security-updates-cisco-and.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-vulnerabilities-in-vrealize-network-analytics-tool/
VMware	https://kb.vmware.com/s/article/92684