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

CYBER GUIDANCE ISSUE 0310

CISCO & VMWARE PATCH CRITICAL FLAWS

DATE ISSUED: 24th April 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Cisco and VMware have released security updates to address critical security flaws in their products that malicious actors could exploit to execute arbitrary code on affected systems.

BREAKDOWN

With a CVSS score of 9.9, the first severe vulnerability is tracked as CVE-2023-20036. A command injection flaw in the web-based user interface of the Cisco Industrial Network Director was is triggered by an improper input validation when uploading a Device pack. Another critical flaw in the Modelling Labs platform with a CVSS score of 9.2 is being tracked as CVE-2023-20154 In which an unauthenticated attacker could access the web interface with administrative privileges, however, valid user credentials are required to exploit this vulnerability.

VMware also released a security patch for a critical deserialisation flaw impacting multiple versions of Aria Operations for Logs (CVE-2023-20864, CVSS score: 9.8). The Log tool helps manage terabytes worth of application and infrastructure logs in large-scale environments. An attacker with access to VMware Aria Operations for logs could execute arbitrary code as root in a low-complexity attack that doesn't require user interaction.

REMEDIATION STEPS

- Upgrade to the latest Cisco version, 2.5.1.
- Upgrade to VMware Aria Operations for Logs 8.12.
- Use vendor-provided hardening guidance to ensure your configuration has the strongest possible security controls in place.
- Network monitoring and analysis should be conducted regularly to detect and investigate anomalous network behaviour.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/vmware-fixes-vrealize-bug-that-let-attackers-run-code-as-root/

The Hacker News https://thehackernews.com/2023/04/cisco-and-vmware-release-security.html