UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00111

## CISCO RCE FLAW IN NEXUS SWITCHES

**DATE ISSUED:** 2nd March 2021

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

## OVERVIEW

A critical vulnerability ranking 10/10 on the CVSS scoring, allowing Remote Code Execution (RCE) affecting the Nexus 3000 and 9000 models of Cisco network switches has been remedied by Cisco this week. CVE-2021-1388.

## BREAKDOWN

This is one of three vulnerabilities patched by Cisco this week. By bypassing the authentication in the intersite policy manager, attackers may be able to access the aforementioned Cisco network switches providing them access. The issue stems from Cisco's management software for business and policy management tool - ACI Multi-Site Orchestrator (MSO) where improper token validation on an API endpoint can be exploited, granting administrative access to the console by sending a well-crafted request. Any ACI MSO running version 3.0 of the software are affected but are only susceptible if deployed on a Cisco Application Service Engine. There are no known public exploits at this time.

The two other known vulnerabilities patched this week include a Root Privilege access flaw CVE-2021-1361 which stems from an incorrectly configured port 9075 which will listen and respond to external connection requests, as well as an Unauthorised Access flaw CVE-2021-1393 affecting the Cisco Application Service Engine Software version 1.1 and earlier.

## REMEDIATION STEPS

- Apply all security patches issued by Cisco this week and last.
- Monitor network activity and network devices for anomalous behaviours.

## REFERENCES & RESOURCES

Threatpost https://threatpost.com/cisco-critical-security-flaw/164255/
Security Week https://www.securityweek.com/cisco-patches-severe-flaws-network-management-products-switches