مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Cisco Meeting Management REST API

Tracking #:432316776

Date:23-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the REST API of Cisco Meeting Management, which could potentially allow a remote, authenticated attacker with low privileges to escalate their privileges to an administrator level on affected systems.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the REST API of Cisco Meeting Management, which could potentially allow a remote, authenticated attacker with low privileges to escalate their privileges to an administrator level on affected systems.

- CVE Identifier: **CVE-2025-20156**
- CVSS Base Score: 9.9 (Critical)
- This vulnerability exists because proper authorization is not enforced upon REST API users. An attacker could exploit this vulnerability by sending API requests to a specific endpoint. A successful exploit could allow the attacker to gain administrator-level control over edge nodes that are managed by Cisco Meeting Management.

Affected Products

- Cisco Meeting Management (All versions up to 3.9)
- Cisco Meeting Management versions 3.8 and earlier

Products Not Affected

- Cisco Meeting Management version 3.10 and later

Fixed Versions:

- For versions 3.8 and earlier: Migrate to a fixed release.
- For version 3.9: Update to version 3.9.1 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Cisco Meeting Management versions to Fixed Software Versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc