مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Static SSH Credential Vulnerability in Cisco Unified CM

Tracking #:432317440

Date:03-07-2025

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

TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has disclosed a critical remote code execution vulnerability (CVE-2025-20309, CVSS 10.0) affecting Cisco Unified Communications Manager (Unified CM) and Session Management Edition (SME).

## TECHNICAL DETAILS:

Cisco has disclosed a critical remote code execution vulnerability (CVE-2025-20309, CVSS 10.0) affecting Cisco Unified Communications Manager (Unified CM) and Session Management Edition (SME). The flaw arises from static, undeletable root SSH credentials inadvertently included in Engineering Special (ES) software releases, enabling unauthenticated, remote attackers to gain root-level access and fully compromise the affected systems.
No workarounds exist, and Cisco strongly advises affected users to immediately upgrade to 15SU3 (released July 2025) or apply the provided patch.

**Vulnerability Details:**

- **CVE ID:CVE-2025-20309**
- **CVSS Score**: **10.0 (Critical)**
- **Vulnerability Type**: Use of static, hard-coded SSH credentials (CWE-798)
- **Affected Products**:
  - Cisco Unified Communications Manager (Unified CM)
  - Cisco Unified CM Session Management Edition (SME)
  - Specifically **Engineering Special (ES)** releases:
    - Versions **15.0.1.13010-1 through 15.0.1.13017-1**
- **Unaffected Versions**:
  - Unified CM/SME **12.5 and 14**
  - Other Service Updates (SUs) are not impacted
- **CVSS Vector**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- **Attack Vector**:
  - **Remote** attacker
  - **No authentication required**
  - Access via **SSH using root credentials**
- **Cause**:
  - **Static root account** credentials left from development
  - Credentials cannot be changed or deleted by users
- **Impact**:
  - Full **root-level access** to affected systems
  - Ability to **execute arbitrary commands**
  - Complete **system compromise**
- **Exploit Status**:
  - **No public exploitation reported** as of July 2, 2025
- **Workaround**: **None available**
- **Patch / Fix**:
  - Upgrade to **Unified CM/SME 15SU3**
  - Or apply patch: ciscocm.CSCwp27755_D0247-1.cop.sha512

**Indicators of Compromise:**

Successful exploitation would result in a log entry to /var/log/active/syslog/secure for the root user with root permissions. Logging of this event is enabled by default.

To retrieve the logs, run the following command from the CLI:

cucm1# file get activelog syslog/secure
If a log entry both includes sshd and shows a successful SSH login by the user root, it is an IoC, as shown in the following example:

Apr 6 10:38:43 cucm1 authpriv 6 systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Apr 6 10:38:43 cucm1 authpriv 6 sshd: pam_unix(sshd:session): session opened for user root by (uid=0)

## RECOMMENDATIONS:

- Apply Security Patch Immediately: Upgrade affected systems to Cisco Unified CM/SME 15SU3 (July 2025)
- Check for Indicators of Compromise (IoCs) and Enable real-time monitoring for privileged access and root logins.
- Set up alerts for unusual behavior on Unified CM systems.
- Stay Informed: Regularly monitor Cisco Security Advisories

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-cucm-ssh-m4UBdpE7