Cisco Unified CM Vulnerability Opens Door for Full System Takeover

TL;DR

Cisco has publicized a critical vulnerability (CVE-2025-20309, CVSS 10) in certain versions of Cisco Unified Communications Manager (Unified CM) and Session Management Edition (SME).

The flaw involves static, undeletable root credentials that could let a remote attacker take full control of the system. There are no workarounds. Users should patch immediately.

Overview

Cisco discovered a serious security issue affecting specific Engineering Special (ES) releases of Unified CM and Unified CM SME. The vulnerability (CVE-2025-20309, CVSS 10) stems from hard-coded root credentials left over from development.

An unauthenticated attacker could exploit this weakness to log in over SSH as root and run any command they choose. There is no way to change or remove these static credentials.

Affected Versions

- Unified CM and Unified CM SME ES 15.0.1.13010-1 through 15.0.1.13017-1

If CVE-2025-20309 is exploited, attackers could gain root access without credentials, run arbitrary commands, and fully compromise systems. The presence of static root credentials in production software gives attackers direct access without the usual barriers. This type of flaw removes the need for complex intrusion methods. If your environment includes an affected ES build, apply the patch immediately. Leaving this unaddressed provides attackers with an easy path to full system control.

Aspire Protects

- **Patch** - Apply Cisco's software updates. Find patch guidance in Cisco's advisory.
- Review /var/log/active/syslog/secure for any successful SSH logins as root.
- Make sure that only trusted administrative networks can reach the management interfaces.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may have used the static root account to gain access.

Execution

- Command and Scripting Interpreter [T1059] – The attacker could run arbitrary commands once logged in as root.

Persistence

- Account Manipulation [T1098] – The attacker may create new privileged accounts after access.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations across all sectors using Cisco Unified CM or Unified CM SME could be impacted, particularly:

- Telecommunications
- Education
- Healthcare
- Government
- Finance

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Unified Communications Manager Static SSH Credentials Vulnerability

NVD - CVE-2025-20309