Cisco Unified CM Vulnerability Now Being Exploited in the Wild

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A high-severity vulnerability in Cisco Unified Communications Manager (CVE-2026-20230, CVSS 8.6) is being actively exploited in the wild.

The flaw may allow an unauthenticated attacker to write files to the underlying operating system and ultimately obtain root privileges on affected systems.

Overview

There is a high-severity vulnerability (CVE-2026-20230, CVSS 8.6) in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME). These products are commonly used by organizations to manage voice, video, and unified communications services.

Affected Products

- Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) Release 14 prior to 14SU6.
- Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) Release 15 prior to 15SU5 or COP1 patch.

Note: Systems are only vulnerable if the Cisco WebDialer Web Service is enabled. WebDialer is disabled by default.

CVE-2026-20230 allows an unauthenticated attacker to send crafted HTTP requests to an affected system. Successful exploitation may allow an attacker to write files to the underlying operating system and gain root privileges.

Cisco released security updates for the vulnerability, but it is now being actively exploited and proof-of-concept exploit code is publicly available. While this vulnerability does not directly affect firewalls, a compromised Unified CM server may provide access to additional systems within the environment. Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Upgrade affected systems to Cisco Unified CM Release 14SU6 or later. See Cisco's advisory for more information.
    - Apply the Cisco COP1 patch if running Cisco Unified CM Release 15.
- Determine whether the Cisco WebDialer Web Service is enabled.

    - Disable the Cisco WebDialer Web Service if it is not required for business operations.
- Review system logs for suspicious HTTP requests and unauthorized file creation activity.
- Monitor affected systems for signs of privilege escalation or unauthorized administrative access.

TTPs

Initial Access

- Exploit Public-Facing Application (T1190) – An attacker may exploit a vulnerable internet-facing Unified CM WebDialer service to gain access to the affected system.

Privilege Escalation

- Exploitation for Privilege Escalation (T1068) – Successful exploitation may allow an attacker to gain root privileges on the affected system.

IoCs

Observed file:

- `/tmp/cve-2026-20230-test.txt`

Observed activity:

- Crafted HTTP requests targeting the Cisco WebDialer service
- File creation attempts on vulnerable Unified CM systems
- Use of file:// URIs to write files to the underlying operating system
- Reconnaissance activity to identify vulnerable devices

Aspire is actively monitoring this threat and will notify customers if additional indicators become available.

Targeted Industries

Organizations using Cisco Unified CM or Cisco Unified CM SME may be affected, especially those in:

- Education
- Healthcare
- Public Sector
- Finance
- Retail
- Energy

- Manufacturing

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 Server-Side Request Forgery Vulnerability