Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Unified Communications Products Critical Vulnerability

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	11
Authors	Vlad Dumitrescu <vlad.dumitrescu@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-01-22
Issue Date	2026-01-22

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A vulnerability has been discovered in Cisco Unified Communications Products which could allow for remote code execution. Cisco Unified Communications (UC) Products are an integrated suite of IP-based hardware and software that combine voice, video, messaging, and data into a single platform. Successful exploitation of this vulnerability could allow for remote code execution as root, which may lead to the complete compromise of the affected device.

Risk

Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Technical summary

A vulnerability has been discovered in Cisco Unified Communications Products which could allow for remote code execution. Details of the vulnerability are as follows:

Tactic: Initial Access (TA0001):
Technique: Exploit Public-Facing Application (T1190):

- A vulnerability in Cisco Unified Communications Products which could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending a sequence of crafted HTTP requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. (CVE-2026-20045)

Successful exploitation of this vulnerability could allow for remote code execution as root, which may lead to the complete compromise of the affected device.

Threat Intelligence

The Cisco PSIRT is aware of attempted exploitation of CVE-2026-20045 in the wild.

Systems Affected

- Unified CM (CSCwr21851)
- Unified CM SME (CSCwr21851)
- Unified CM IM&P (CSCwr29216)
- Unity Connection (CSCwr29208)
- Webex Calling Dedicated Instance (CSCwr21851)

Recommendations

Smarttech247 team recommend the following actions to be taken:

- Apply appropriate updates provided by Cisco or other vendors which use this software to vulnerable systems immediately after appropriate testing. **(M1051: Update Software)**
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and

excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. **(M1026: Privileged Account Management)**
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. **(M1016: Vulnerability Scanning)**
    - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. **(M1030: Network Segmentation)**
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. **(M1050: Exploit Protection)**

- Safeguard 10.5: Enable Anti-Exploitation Features: Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-20045

CVEs

CVE-2026-20045

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com