Cisco Patches Critical Vulnerability in Contact Center Products

By Ionut Arghire on January 13, 2022

Cisco on Wednesday announced patches for a critical vulnerability in Unified Contact Center Management Portal (Unified CCMP) and Unified Contact Center Domain Manager (Unified CCDM) that could be exploited remotely to elevate privileges to administrator.

Tracked as CVE-2022-20658 (CVSS score of 9.6), the issue exists because there was no server-side validation of user permissions, which allowed an attacker to submit a crafted HTTP request to exploit the bug on a vulnerable system.

“A successful exploit could allow the attacker to create Administrator accounts. With these accounts, the attacker could access and modify telephony and user resources across all the Unified platforms that are associated to the vulnerable Cisco Unified CCMP,” Cisco explains.

The company also notes that an attacker would need to have valid Advanced User credentials to successfully exploit the vulnerability.

Cisco Unified CCMP and Unified CCDM running with the default settings are impacted by the bug, Cisco explains.

The security flaw was addressed with the release of Unified CCMP/ Unified CCDM versions 11.6.1 ES17, 12.0.1 ES5, and 12.5.1 ES5. Version 12.6.1 of the software is not affected.

Cisco says it is not aware of the vulnerability being exploited in malicious attacks.

On Wednesday, the tech company also announced the release of patches for eight medium-severity vulnerabilities in Tetration, Secure Network Analytics, Prime Access Registrar Appliance, Prime Infrastructure (PI) and Evolved Programmable Network Manager (EPNM), several IP Phone models, Enterprise Chat and Email (ECE), Security Manager, and Adaptive Security Device Manager (ASDM).

Detailed information on the patched flaws is available on Cisco's security portal.

Related: Cisco Plugs Critical Holes in Catalyst PON Enterprise Switches

Related: Cisco Patches High-Severity Vulnerabilities in Security Appliances, Business Switches

Related: Cisco Patches Critical Vulnerabilities in IOS XE Software

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

FCC Chair Proposes New Policies for Carrier Data Breach Reporting
Cisco Patches Critical Vulnerability in Contact Center Products
U.S. Cyber Command Officially Links MuddyWater Group to Iranian Intelligence
Mozilla Patches High-Risk Firefox, Thunderbird Security Flaws
Microsoft Introduces New Security Update Notifications

Tags:

NEWS & INDUSTRY Vulnerabilities