CYBER ADVISORY

TLP:CLEAR

25 January 2024

Cisco Communications Software Vulnerability

CVE-2024-20253 | RCE | Cisco | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-20253.[1] The vulnerability affects several of Cisco Unified Communications Manager (CM) and Contact Center Solutions products.[2] The remote code execution (RCE) vulnerability could allow an attacker to execute arbitrary code on an affected device.[3,4]

Affected Cisco Product
Packaged Contact Center Enterprise (PCCE)
Unified Communications Manager (Unified CM)
Unified Communications Manager IM & Presence Service (Unified CM IM&P)
Unified Communications Manager Session Management Edition (Unified CM SME)
VMware Cloud Foundation (Aria Automation)
Unified Contact Center Enterprise (UCCE)
Unified Contact Center Express (UCCX)
Unity Connection
Virtualized Voice Browser (VVB)

Table 1: Vulnerable Cisco Software

The Cal-CSIC recommends immediately applying the appropriated patch to the affected Cisco software.

For further information on applying patches, please refer to Cisco Security Center.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Cisco warns of critical RCE flaw in communications software;" https://www.bleepingcomputer.com/news/security/cisco-warns-of-critical-rce-flaw-in-communications-software/; accessed 25 January 2024
[2] IT News; "Cisco unified comms systems patched against RCE;" https://www.itnews.com.au/news/cisco-unified-comms-systems-patched-against-rce-604400; accessed 25 January 2024
[3] Vul DB; "Cisco Packaged Contact Center Enterprise Remote Code Execution;" https://vuldb.com/?id.251994; accessed 25 January 2024
[4] Cisco; "Cisco Unified Communications Products Remote Code Execution Vulnerability;" https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm; accessed 25 January 2024