Security Advisory 2024-015

Remote Code Execution Vulnerability in Cisco Products

January 29, 2024 — v1.0

TLP:CLEAR

History:

- *29/01/2024 — v1.0 – Initial publication*

Summary

On January 24, 2024, Cisco disclosed a critical vulnerability in multiple the Unified Communications and Contact Center Solutions products [1]. This vulnerability, tracked as `CVE-2024-20253` with a CVSS score of 9.9, could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. Currently, Cisco has no evidence of public proof of concept exploits for this vulnerability or active exploitation in the wild.

Technical Details

This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.

Affected Products

This vulnerability affects the following Cisco products in the default configuration [2]:

- Unified Communications Manager (Unified CM), versions 11.5, 12.5(1), and 14.
- Unified Communications Manager IM & Presence Service (Unified CM IM&P), versions 11.5(1), 12.5(1), and 14.
- Unified Communications Manager Session Management Edition (Unified CM SME), versions 11.5, 12.5(1), and 14.
- Unified Contact Center Express (UCCX), versions 12.0 and earlier and 12.5(1).
- Unity Connection, versions 11.5(1), 12.5(1), and 14.
- Virtualized Voice Browser (VVB), versions 12.0 and earlier, 12.5(1), and 12.5(2).

Recommendations

CERT-EU recommends updating to the latest version of the affected product as soon as possible to mitigate this vulnerability [2].

References

[1] https://www.bleepingcomputer.com/news/security/cisco-warns-of-critical-rce-flaw-in-communications-software/

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm