Security Advisory 2024-005

Critical Vulnerability in Cisco Unity Connection

January 11, 2024 — v1.0

TLP:CLEAR

History:

- *11/01/2024 — v1.0 – Initial publication*

Summary

On January 10, 2024, Cisco disclosed a critical vulnerability in its Unity Connection product [1]. This vulnerability, tracked as `CVE-2024-20272` with a CVSS score of 7.3, could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. 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 a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.

Affected Products

The following versions are affected [2]:

- 12.5 and earlier, before the first fixed release (`12.5.1.19017-4`)
- 14 before the first fixed release (`14.0.1.14006-5`)

Recommendations

CERT-EU recommends updating to the latest version of Cisco Unity Connection as soon as possible to mitigate this vulnerability.

References

[1] https://www.bleepingcomputer.com/news/security/cisco-says-critical-unity-connection-bug-lets-attackers-get-root/

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD#fs