January 11, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- Cisco Unity Connection (ISE) – versions prior to 12.5.1.19017-4 and 14.0.1.14006-5

Technical Details

A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system.
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.*

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- **CVE-2024-20272, CVE-2024-21887, CVE-2024-20272, CVE-2023-20248, CVE-2023-20249, CVE-2024-20277, CVE-2024-20287, CVE-2023-20257, CVE-2023-20258, CVE-2024-20270, CVE-2024-20251, CVE-2023-20193, CVE-2023-20194**
- Cisco Advisory – cisco-sa-cuc-unauth-afu-FROYsCsD
- Cisco Security Advisories