June 12, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple vulnerabilities in the web-based management interface of Cisco Finesse. These vulnerabilities affected Cisco Finesse in the default configuration. Additionally, Cisco products bundled with Cisco Finesse are also affected by these vulnerabilities: Packaged Contact Center Enterprise (Packaged CCE), Unified Contact Center Enterprise (Unified CCE), Unified Contact Center Express (Unified CCX) and Unified Intelligence Center.

Multiple vulnerabilities in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to perform a stored cross site-scripting (XSS) attack by exploiting a remote file inclusion (RFI) vulnerability or perform a server-side request forgery (SSRF) attack an affected system.

Technical Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit the other vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerability.

A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.

This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device.

A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability.

This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-20404, CVE-2024-20405
- Cisco Finesse Web-Based Management Interface Vulnerabilities
- VRM Vulnerability Reports