

Overall rating: Medium



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in Cisco Emergency Responder, Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection. The vulnerability affects Emergency Responder, Unified CM, Unified CM SME and Unity Connection.

Technical Details

A vulnerability in Cisco Emergency Responder, Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an authenticated, remote attacker to elevate privileges to root on an affected device.

This vulnerability exists because the application does not properly restrict the files that are being used for upgrades. An attacker could exploit this vulnerability by providing a crafted upgrade file. A successful exploit could allow the attacker to elevate privileges to root. To exploit this vulnerability, the attacker must have valid platform administrator credentials on an affected device.

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: High

User Interaction: None

This vulnerability is rated as a **MEDIUM** 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.

References

- CVE-2023-20266
- [Cisco Unified Communications Products Privilege Escalation Vulnerability](#)
- [Cisco Security Advisories](#)

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here:
<https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx>

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca