December 1, 2023

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 the web-based management interface of a small subset of Cisco IP Phones. The vulnerability affects IP DECT 110 Single-Cell Base Station with Multiplatform Firmware, IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware, Unified IP Phone 6901 and Unified SIP Phone 3905 versions if they were running a vulnerable release of Cisco IP Phone Software.

Technical Details

A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
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-2023-20265
- Cisco IP Phone Stored Cross-Site Scripting Vulnerability
- VRM Vulnerability Reports