August 9, 2024

Overall Rating: Critical

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 Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an attacker to execute arbitrary commands on the underlying operating system or cause a denial of service (DoS) condition. The vulnerability affects versions that run on Cisco Small Business SPA300 Series and Cisco Small Business SPA500 Series IP Phones, regardless of the configuration.

Technical Details

Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system with root privileges.

These vulnerabilities exist because incoming HTTP packets are not properly checked for errors, which could result in a buffer overflow. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to overflow an internal buffer and execute arbitrary commands at the root privilege level.

Cisco has not released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** 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-2024-20450, CVE-2024-20451, CVE-2024-20452, CVE-2024-20453, CVE-2024-20454
- Cisco Small Business SPA300 Series and SPA500 Series IP Phones Web UI Vulnerabilities
- VRM Vulnerability Reports