مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Cisco IP Phones

Tracking #:432316130

Date:08-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been identified in the web-based management interface of Cisco Small Business SPA300 and SPA500 Series IP Phones.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in the web-based management interface of Cisco Small Business SPA300 and SPA500 Series IP Phones. These vulnerabilities could allow unauthenticated remote attackers to execute arbitrary commands on the underlying operating system or cause a denial of service (DoS) condition. **Cisco has not released updates and will not release software updates or workarounds to address these vulnerabilities, and the affected products are approaching their end-of-life status.**

- **Affected Products**: Cisco Small Business SPA300 Series and SPA500 Series IP Phones across all software releases.
- **Vulnerability Details:**
  1. **CVE-2024-20450, CVE-2024-20452, CVE-2024-20454 CVSS Base Score: 9.8**: Arbitrary Command Execution Vulnerability, allowing attackers to execute commands with root privileges due to improper error checking of incoming HTTP packets.
  2. **CVE-2024-20451, CVE-2024-20453**: **CVSS Base Score: 7.5**- DoS Vulnerability, which may cause affected devices to reload unexpectedly by sending crafted HTTP packets.

RECOMMENDATIONS:

- **Immediate Action**: Assess whether the Cisco Small Business SPA300 or SPA500 Series IP Phones are in use. If so, advise immediate reconsideration of their deployment in the network.
- **Migration Strategy**: Plan for the migration to supported products that meet current security standards. Consult Cisco's security advisories regularly for guidance on vulnerabilities and upgrade solutions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz