مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Cisco IP Phone High-Severity Vulnerabilities

Tracking #:432315815

Date:03-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in Cisco IP Phone firmware that could allow an unauthenticated, remote attacker to compromise affected devices. These vulnerabilities could be exploited to cause a denial-of-service (DoS) condition, gain unauthorized access to the device, or view sensitive information.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-20376: Cisco IP Phone DoS Vulnerability**
  - **High Severity, CVSS Base Score: 7.5**
  - Description: A vulnerability in the web-based management interface allows attackers to cause an affected device to reload, leading to a Denial-of-Service (DoS) condition.
  - Cause: Insufficient validation of user-supplied input.
  - Exploitation: Attackers can send a specially crafted request to the web interface.
- **CVE-2024-20378: Cisco IP Phone Information Disclosure Vulnerability**
  - **High Severity, CVSS Base Score: 7.5**
  - Description: A vulnerability in the web-based management interface allows attackers to retrieve sensitive information from affected devices.
  - Cause: Lack of authentication for specific endpoints.
  - Exploitation: Attackers can connect to the affected device to potentially steal user credentials, record traffic, or eavesdrop on VoIP calls.
- **CVE-2024-20357: Cisco IP Phone Unauthorized Access Vulnerability**
  - **Medium Severity, CVSS Base Score: 5.3**
  - Description: A vulnerability in the XML service allows attackers to initiate phone calls on affected devices.
  - Cause: Improper bounds-checking during XML request parsing.
  - Exploitation: Attackers can send a crafted XML request to the device.

Affected Products:

- IP Phone 6800 Series with Multiplatform Firmware
- IP Phone 7800 Series with Multiplatform Firmware
- IP Phone 8800 Series with Multiplatform Firmware
- Video Phone 8875 in Multiplatform Mode

Mitigations:

- **IP Phone 6800, 7800, and 8800 Multiplatform Firmware**

Cisco Multiplatform Firmware Release	First Fixed Release
12.0.4 and earlier	12.0.4SR1

- **Video Phone 8875**

Cisco PhoneOS Release	First Fixed Release
2.3.1.001 and earlier	2.3.1.0101

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Cisco.

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-ipphone-multi-vulns-cXAhCvS