مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco BroadWorks SIP Denial of Service Vulnerability

Tracking #:432316781

Date:24-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in Cisco BroadWorks, affecting its SIP (Session Initiation Protocol) processing subsystem.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in Cisco BroadWorks, affecting its SIP (Session Initiation Protocol) processing subsystem. This vulnerability allows unauthenticated, remote attackers to send a high volume of specially crafted SIP requests that could exhaust system memory on the affected servers, causing a Denial of Service (DoS) condition.

Vulnerabilities Overview:

- **CVE-ID-CVE-2025-20165**
- **CVSS Score:** Base 7.5
- Affected Products: Cisco BroadWorks (all configurations)
- Fixed Software: Software updates are available and should be applied immediately.
- The vulnerability can be exploited remotely, without authentication, by sending specially crafted SIP requests.

Fixed Versions:

- Cisco BroadWorks Release Independent version RI.2024.11 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Cisco BroadWorks to the fixed version.

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-bw-sip-dos-mSySbrmt