CVE-2025-20236: CISCO WEBEX APP REMOTE CODE EXECUTION

Vairav CVE Report

Date: April 17, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cisco has released a security update to address a high-severity remote code execution (RCE) vulnerability in its Webex App, tracked as **CVE-2025-20236**. The flaw arises from insufficient input validation in the app's custom URL parsing. Exploitation of the vulnerability could allow unauthenticated attackers to execute arbitrary commands on a user's device via a malicious meeting invite link. Cisco has issued fixes in updated versions of the Webex App, and users are urged to upgrade immediately.

VULNERABILITY DETAILS

CVE-2025-20236: Cisco Webex App Remote Code Execution via Malicious Meeting Links

Description: A vulnerability in the custom URL parser of Cisco Webex App allows an unauthenticated, remote attacker to persuade a user to click on a malicious meeting invite link. When clicked, this link triggers the download of arbitrary files that may lead to remote code execution on the user's system. The flaw exists due to insufficient input validation in the Webex App's custom URL handler.

Impact: Remote code execution with the privileges of the targeted user.

CVSS Score: 8.8 (High)

Exploitation: By tricking a user into clicking a crafted Webex link, an attacker can initiate the download and execution of arbitrary files, allowing them to run commands on the user's system without authentication.

AFFECTED PRODUCTS/VERSIONS

- Cisco Webex App Version 44.5 and earlier: Not vulnerable
- Version 44.6: Vulnerable – Fixed in version 44.6.2.30589
- Version 44.7: Vulnerable – Must migrate to a fixed release
- Version 44.8 and later: Not vulnerable

RECOMMENDATIONS

- Upgrade immediately to version 44.6.2.30589 or later.
- Users running version 44.7 should migrate to a newer, fixed version.

- Regularly monitor Cisco PSIRT advisories for future vulnerabilities.
- Educate users about phishing risks and avoid clicking on suspicious links.

REFERENCES

https://securityonline.info/cisco-patches-cve-2025-20236-unauthenticated-rce-flaw-in-webex-app-via-malicious-meeting-links/

https://www.cve.org/CVERecord?id=CVE-2025-20236

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-client-rce-ufyMMYLC

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com