Cisco Webex App – Client-Side Remote Code Execution Vulnerability

Overview

A high-severity vulnerability (CVE-2025-20236, CVSS 8.8) in the Cisco Webex App could let a remote, unauthenticated attacker execute arbitrary code on a user's machine. The flaw stems from improper input validation in the app's custom URL parser.

If exploited, an attacker could send a malicious meeting invite link that prompts a user to download an arbitrary file, leading to code execution under the user's privileges.

Affected products

- Cisco Webex App Releases:
  - 44.6 (vulnerable) fixed in 44.6.2.30589
  - 44.7 (vulnerable) must migrate to a fixed release
  - 44.5 and earlier / 44.8 and later (not vulnerable)

The issue lies in how the Webex App processes meeting invite links. By crafting a malicious URL, attackers can trick users into downloading and executing unauthorized files. The vulnerability affects all platforms running Cisco Webex App, regardless of configuration or operating system. It does not require prior access or privileges, making exploitation relatively easy.

Cisco Webex is a staple in many organizations, especially in education, healthcare, finance, and legal sectors. This vulnerability shows how even trusted collaboration tools can become attack vectors when input validation is weak. If Webex is part of your workflow, please patch immediately.

Aspire Protects

- **Patch –** Upgrade to the latest patched version(s). You may find patch guidance in Cisco's advisory.
- Ensure software upgrade policies include regular Webex updates, especially in environments that rely heavily on collaboration tools.
- Train users to avoid clicking on unexpected or unfamiliar meeting links, especially from unknown sources.

TTPs to Watch

Initial Access

- Phishing: Spearphishing Link [T1566.002] – The attacker may have sent a malicious Webex meeting invite to trick the user into clicking the link and downloading a harmful file.

Execution

- User Execution [T1204] – The attacker relied on user interaction to initiate the download and run the file.

Impact

- Inhibit System Recovery [T1490] – If used with ransomware or malware payloads, this access path could disrupt system recovery.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations across several industries may be impacted due to widespread use of Cisco Webex for communication and collaboration.

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government
- Energy

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Webex App Client-Side Remote Code Execution Vulnerability

NVD - CVE-2025-20236