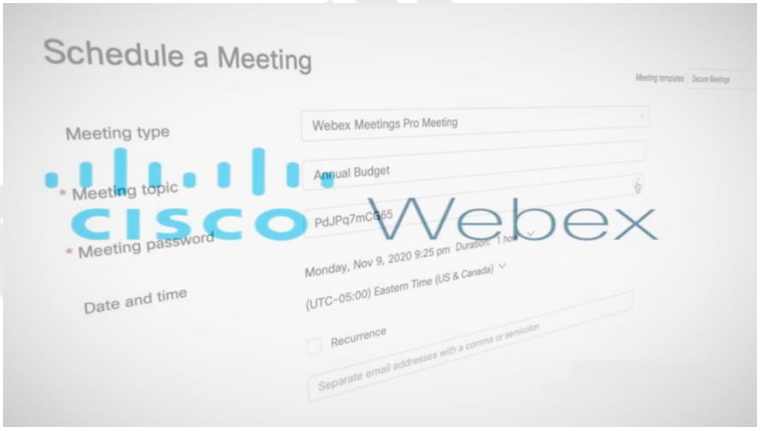
SEQURETEK

Cisco Webex Flaws

OVERVIEW

Cisco's Webex video conferencing application could be exploited to join meetings as ghost users, in without the knowledge of other meeting participants or the host. An attacker could exploit one of the flaws to access the names, email addresses, and IP addresses of meeting participants. Another flaw could be exploited to remain in a meeting even after being dismissed by the host.



OVERVIEW

- Cisco **patched three vulnerabilities discovered by IBM researchers**, in the **Webex** video conferencing app that could allow attackers to sneak in and **privately join Webex meetings as ghost users** without being seen by the organizer or any of the attendees.
- Ghost users can hear, speak, and share media in the joined meeting without being invited.
- These flaws affect both scheduled meetings with unique meeting URLs and Webex Personal Rooms in MacOS, Windows, and the iOS version of Webex Meetings applications and Webex Room Kit appliance.
- Malicious actors could abuse following the vulnerabilities to join a meeting without being seen.
    - **CVE-2020-3441**(CVSS score 5.3) - **Cisco Webex Meeting Information Disclosure Vulnerability.**

      This vulnerability is due to insufficient protection of sensitive participant information.
    - **CVE-2020-3471**(CVSS score 6.5) - **Cisco Webex Meetings and Cisco Webex Meetings Server Audio Information Exposure Vulnerability.**

      This vulnerability is due to a synchronization issue between meeting and media services on a vulnerable Webex site.
    - **CVE-2020-3419**(CVSS score 6.5) - **Cisco Webex Meetings and Cisco Webex Meetings Server Information Disclosure Vulnerability.**

      This vulnerability is due to the improper handling of authentication tokens by a vulnerable Webex site.

TECHNICAL DETAILS

- These vulnerabilities could be exploited with a **combination of social engineering**, **open source intelligence (OSINT)** and **cognitive overloading techniques**.
- All three vulnerabilities work by **exploiting the handshake process** that Webex uses to establish a connection between meeting participants.
- By **manipulating join messages in handshake process between the Webex client application and the Webex server back-end,** attacker could stay in a meeting without being seen by others.

- This works because of improper handling of the values by the server and other participants' client applications.
- Successful exploitation of these vulnerabilities allows an attacker to:
  - **Join a meeting as a ghost,** in most cases with full access to audio, video, chat, and screen-sharing capabilities (CVE-2020-3419)
  - **Maintain an audio feed as a ghost even after being expelled** by the meeting host. (CVE-2020-3471)
  - **Access full names, email addresses, and IP addresses** of meeting attendees, even when not admitted to a conference room. (CVE-2020-3441)
- Cisco has since patched cloud-based Cisco Webex Meetings sites and released security updates for on-premises software such as the Cisco Webex Meetings mobile app and the Cisco Webex Meetings Server software.

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Update to the latest version of Webex.
  - Before selecting and implementing your collaboration tool (like Webex) within an organization, test the security of the tools to ensure secure and properly configured use across the organization.
  - Employees should evaluate their meetings' sensitivity when it is first scheduled. This can help to determine what security practices are needed.
  - Use unique meeting ID instead of the standard personal meeting room name.
  - Use passwords or PINs so only invited participants can enter your meeting. Use strong passwords. Request that your invited participants do not forward the invitation further.
  - Do not publish passwords to public-accessible websites.
  - Do not share your Audio PIN with anyone.
  - Start calls with a simple roll call to ensure you know who is on the call. This can help to identify participants using their phone numbers instead of a profile name, similar to what non-member meetings allow.
  - Keep tabs on notifications of who enters the meeting room and take advantage of both visual and audio notifications, so nothing goes unnoticed.
  - Set meetings to automatically lock at the beginning of each call. This will require attendees to request admittance to enter the room before joining.

- When you have back-to-back meetings in the same room, make sure to start a fresh meeting between each call.

- **Corrective Actions**
  - If your meeting has been compromised, end it immediately. Notify and mute all participants so they are aware of the situation and to not divulge any further information.
  - Report the issue to the platform vendor and report it to your company's security team.

About Sequretek

Sequretek is an India headquartered cybersecurity firm with customers across North America, Europe, Africa, the Middle East, and India. It is amongst the very few companies who has end to end cyber-security offerings in the areas of Endpoint Security, Identity Access Governance, Threat Intelligence, Security Monitoring, and Security Management. Sequretek has been recognized as the "Security Product Company of Year" by the Data Security Council of India (DSCI) and was also featured in the list of Top 500 - Fastest Growing Companies in Asia Pacific Region published by Financial Times and Statista. Sequretek has been successful in securing the IT assets of over 100 clients across Banking, Financial Services, Insurance, Manufacturing, Pharmaceuticals, Services, Retail, and Logistics sectors.

Simplify Security | Cutting Edge Technologies for Next Generation Threats | Reduce Total Cost of Ownership

Feel free to reach out at info@sequretek.com to know more about our products or to see a live demonstration of our products.