Possible Solution

Relevance

Kind of affected systems

Desktop, end user systems with Windows OS. Cisco Webex Meetings Desktop App and Cisco Webex Productivity Tools releases earlier than releases 40.6 and 40.10

Placement

Accessability of end user systems, internet uplink

Authentication

Strength of authentication mechanisms

Usecases

Employees who work from a shared computer, stay logged into their computers and use WebEx

Threats

Authentication strength

Single factor authentication combined with weak password policies (length, complexity) so that an attacker can easily gain access

User awareness

Bad awareness and behavior of end users leading to login possibilities for attackers

Credential management

Weak credential management, an attacker becomes aware of valid credentials of a Windows end-user system, e.g. password leaks

Malware

Virus auto-running on other user's profile, process starting a session as a different user

Risks

Potential damage

Identity theft, information theft, information disclosure

Probability estimation

Low as an attacker must have valid credentials on the end-user system

Criticality

CVSS Score (5.5) recognized and correct level (Medium)

Criticality

Recommendation timeframe for software update

Countermeasures

- Deploy software update
- Implement strong authentication
- Perform user awareness training
- Disallow access by clients with versions not containing the fix
- Inform all employees with WebEx accounts and ask them to upgrade their installation