Cisco WebEx Meetings Vulnerabilities

Cisco released 3 security patches for vulnerabilities found at their Client and Server of Webex Meetings, the company's Video conferencing application.

One of the vulnerabilities allows malicious actors to stay connected to an audio session (listening and participating) even if they were expelled from the meeting. Another vulnerability requires valid passwords and meeting join links, but if exploited it would allow malicious actors to fully join a session without appearing as a participant. The vulnerability exits in Webex site platform, due to improper handling of users' authentication tokens.
The third vulnerability exists due to insufficient protection on the Webex Roster. A successful exploitation of the vulnerability allows malicious actors, from the meeting lobby, to view and gather participants information such as email addresses, IP Addresses and more.
The third

More details about the vulnerabilities and the patches released can be found at Cisco's security center - CVE-2020-3419, CVE-2020-3441, CVE-2020-3471 –