Zoom Video Communications, Inc.
Public Statement: Predicting Zoom Meeting IDs
October 1, 2019

Recently, Zoom became aware of a concern that Zoom meeting IDs could be predicted by using automated technology to test the validity of thousands of numerical combinations quickly.

In August, Zoom rolled out two pre-planned features that address this specific concern:

- The Zoom website no longer indicates whether a requested meeting ID is valid or invalid, making automated scanning for valid meeting IDs more difficult and time consuming for a bad actor.
- Zoom now detects repeated attempts to scan for meeting IDs and blocks such scans for a period of time.

Additionally, Zoom makes a set of features available to users to control the attendance of their meetings:

- By default, meetings and webinars will not start without the host being present. The host can view their participant list, lock their meeting, and remove participants.
- Additional configurable options include waiting rooms, chime upon entry, and the ability to only allow participants from a specific email domain to join.
- As of September 29, Zoom meetings and webinars are password protected by default, further leveraging an existing feature to prevent unauthorized attendees from joining a meeting. Passwords for meetings and webinars are turned on as the default setting for most account types. Over the next several weeks, remaining account types will be configured to require meeting passwords by default. Users and account administrators are given the option to opt-out of this setting. More information on this new setting can be found at: https://support.zoom.us/hc/en-us/articles/360033331271.

Zoom thanks dedicated security researchers for reporting this concern to our team and helping us to further strengthen the security of our meetings.

###

Zoom Video Communications, Inc.
55 Almaden Blvd, Suite 600, San Jose, CA 95113
zoom.us | 1.888.799.9666