90-Day Security Plan Progress Report: June 24

As we continue on our 90-day plan to improve the security and privacy of our platform, this week's "Ask Eric Anything" webinar focused on recent product security updates, including our efforts surrounding our bug bounty program and the updates coming with the 5.1.1 client release.

Zoom CEO Eric S. Yuan was joined by Zoom President of Product and Engineering Velchamy Sankarlingam, Zoom CPO Oded Gal, and Zoom Head of Product Security Randy Barr.

Zoom CTO Brendan Ittelson, Zoom privacy and security advisor Alex Stamos, and Zoom Deputy General Counsel, Chief Compliance and Ethics Officer Lynn Haaland joined for the Q&A session.

Announcing CISO Jason Lee

Eric started the webinar by announcing that Zoom has hired Jason Lee as our new Chief Information Security Officer, effective June 29, 2020. As the former Senior Vice President of Security Operations at Salesforce and Principal Director of Security Engineering at Microsoft, Lee brings over 20 years of expertise in information security and operating mission-critical services. Jason will play a critical role in helping us build a more secure platform as part of our ongoing effort to improve the security and privacy of our product.

Product updates

This weekend, we will be rolling out our 5.1.1 client and web release, which includes the following changes:

- **Centrally managed virtual backgrounds**: Account admins can manage the virtual backgrounds used by their organization, providing a list of pre-approved backgrounds for users to choose from.
- **Web portal security tab for meeting settings**: The security menu tab will appear in the meeting settings in the web portal, which gathers security-related settings such as passwords, waiting room, and authentication methods into one easy to find place.
- **Updates to Zoom Chat**: Users can hide their presence status from external contacts, and will have the option to prevent external contacts from adding new users to a channel or group chat.

Introducing Velchamy Sankarlingam

Eric introduced Velchamy Sankarlingam, the former Senior Vice President of Cloud Services Development and Operations at VMware, who has joined Zoom as the President of Product and Engineering. As a cloud and collaboration software veteran with over two decades of experience, Velchamy brings a wealth of experience and knowledge to our team and we are excited to have him overseeing our product, engineering, and DevOps team efforts.

New meeting security requirements

Starting July 19, all meetings on paid accounts will be required to either have a Passcode or Waiting Room enabled to ensure safer, more secure meetings. Zoom will enable a Waiting Room for your meetings if neither is enabled. If you already have a Passcode or Waiting Room on, there will be no change to how you schedule meetings. If you add Passcodes to an existing meeting, calendar invites will need to be re-sent to include the Passcode, whereas new meetings that have Passcodes enabled will have the Passcode included in the meeting invite automatically. If Waiting Rooms are enabled, there is no change to how you schedule meetings. Free accounts will continue with current security settings of Passcodes are forced on, and Waiting Rooms are on by default.

Bug Bounty Program Updates

Randy Barr provided a bug bounty and vulnerability

90-Day Security Plan Progress Report: June 24

disclosure program update. As part of our 90-day plan, we have been assessing our internal vulnerability handling processes and the effectiveness of the bug bounty platforms we use. To improve our bug bounty program and our vulnerability disclosure efforts, we have developed a Central Bug Repository and related workflow processes to align with ISO 29147 and 30111. This repository takes inputs from HackerOne, Bugcrowd, and security@zoom.us (the latter of which does not require an NDA) triaged through Praetorian. We established an ongoing review process with daily meetings, and improved our coordination with security researchers and third-party assessors.

Q&A

How do you report a bug bounty to Zoom?

You can send your bug bounty submissions to security@zoom.us, where our dedicated team will review each submission and assign someone to address the issue.

Do you still provide encryption for paid and free accounts?

Yes, all meetings are encrypted with AES 256 bit GCM encryption for both paid and free accounts. We will also make end-to-end encryption of meetings available for free and paid accounts to create a highly secure meeting environment.

Does Zoom ever collect or sell user data?

When customers use our platform, Zoom collects information we need to deliver the service, such as IP addresses; however, Zoom does not and will never sell user data.

Can Zoom add an option for admins to reset Passcode and Waiting Room settings globally?

As an account admin, you can enable or even lock these settings at the account level, which will enable those security settings for all meetings and users by default. You can also enable Passcodes and the Waiting Room at the group or user level.

How does the Waiting Room work?

When the Waiting Room is enabled, participants will be placed into a virtual lobby where the host can review who is trying to join the meeting and admit them, either one by one or all at once. The Waiting Room feature can be enabled at the account, group, user, or meeting level.

Thank you for your support

Thanks for attending this week's session, and thank you to everyone who submitted questions! We truly appreciate your support on our journey to make Zoom the world's most secure enterprise communications platform.

If you missed this week's session, you can watch the recording here.

To give your feedback or to ask Zoom a question, send an email to answers@zoom.us. And be sure to sign up for next week's "Ask Eric Anything" webinar.