Zoom Video Communications, Inc.
Public Statement
July 8, 2019

In March 2019, a security researcher notified Zoom of some concerns related to the Zoom meetings platform. Below we detail those concerns and our responses.

**VIDEO ON VULNERABILITY**

Alleged risk: If an attacker is able to trick a target Zoom user into clicking a web link to the attacker's Zoom meeting ID URL, either in an email message or on an internet web server, the target user could unknowingly join the attacker's Zoom meeting. If the user has not explicitly configured their Zoom client to disable video upon joining meetings, the attacker may be able to view the user's video camera. Because the Zoom client user interface runs in the foreground upon launch, it would be readily apparent to the user that they had unintentionally joined a meeting.

Current state: All first-time Zoom users, upon joining their first meeting from a given device, are asked whether they would like their video to be turned OFF. For subsequent meetings, users can configure their client video settings to turn OFF video when joining a meeting. Additionally, system administrators can pre-configure video settings for supported devices at the time of install or change the configuration at anytime.

Future state: As part of our July 2019 release, Zoom will apply and save the user's video preference from their first Zoom meeting to all future Zoom meetings. Users and system administrators can still configure their client video settings to turn OFF video when joining a meeting. This change will apply to all client platforms.

Related to the alleged video-on vulnerability, the researcher references two issues:

1. **AUTO JOIN VIA ZOOM LOCAL WEB SERVER (MACS ONLY)**
   Zoom installs a local web server on Mac devices running the Zoom client. This is a workaround to an architecture change introduced in Safari 12 that requires a user to accept launching Zoom before every meeting. The local web server automatically accepts the peripheral access on behalf of the user to avoid this extra click before joining a meeting. We feel that this is a legitimate solution to a poor user experience, enabling our users to have seamless, one-click-to-join meetings, which is our key product differentiator.

2. **LOCAL DENIAL OF SERVICE VULNERABILITY (MACS ONLY)**
   The security researcher identified a local denial of service vulnerability. A hacker could have potentially targeted a Mac user who already had the Zoom client installed with an endless loop of meeting join requests, thereby causing the targeted machine to lock up. We have no indication that this vulnerability was ever exploited and we released a fix for it in May 2019.

**ZOOM SECURITY PROGRAM**

Zoom takes all security concerns related to our products very seriously and has a dedicated Security team in place.

Once this particular issue was brought to our Security team's attention, we responded within 1 hour, gathering additional details, and proceeded to perform a risk assessment. Our Security and Engineering teams engaged the researcher and were in frequent contact over a period of several weeks.

We always recommend that security concerns or issues be routed through our 24/7 support team via support.zoom.us  We acknowledge that our website currently doesn't provide clear information for reporting security concerns. As such, in the next several weeks, Zoom will go live with its public bug bounty program, supplementing our existing private program. With the program launch, our website will be updated with a web submission form for all security-related concerns. Non-disclosure on a bug bounty program is common industry practice that provides vendors the flexibility to determine whether or not a vulnerability warrants public disclosure.

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