8 ข้อสรุปปัญหาความปลอดภัยและความเสี่ยงใน Zoom

ที่มา : https://www.i-secure.co.th/2020/04/risk-in-zoom/

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ในหลากหลายอาชีพได้พุ่งเป้าไปยังปัญหาด้านความปลอดภัยในแอปพลิเคชันสำหรับการประชุมออนไลน์ Zoom ซึ่งกำลังได้รับความนิยมอย่างสูงจากสถานการณ์การแพร่ระบาดของ COVIC-19 ผลลัพธ์จากการวิเคราะห์การทำงานและพฤติกรรมของแอปพลิเคชันในหลากหลายแพลตฟอร์มเปิดเผยถึงความเสี่ยงหลายประการที่อาจเกิดขึ้นกับการใช้งานแอปพลิเคชันภายใต้เงื่อนไขต่างๆ

อย่างไรก็ตาม Security ที่ดีไม่ควรเป็น Security ที่เกิดจากความหวาดระแวงอย่างไม่สมเหตุสมผล ดังนั้นในบทความนี้ **ทีมตอบสนองการโจมตีและภัยคุกคาม (Intelligent Response) จากบริษัท ไอ-ซีเคียว จำกัด** จะมาสรุปข่าวที่เกิดขึ้น และความคิดเห็นของเราต่อความเสี่ยงเพื่อให้การจัดการความเสี่ยงนั้นเกิดขึ้นอย่างเหมาะสม

1. ปัญหาความเสี่ยงที่อนุญาตให้ผู้ไม่หวังดีค้นหาและสามารถเข้าร่วมการประชุมเพื่อก่อกวนการประชุมในรูปแบบที่ชื่อ “ZOOMBOMBING”

ระดับความเสี่ยง

สามารถทำให้ผู้ไม่หวังดีใช้ Meeting ID การประชุมเข้าร่วมการประชุมโดยไม่ได้รับอนุญาต และก่อกวนการประชุมด้วยวิธีการต่างๆ

สถานะการแก้ไข

ดำเนินการแก้ไขเรียบร้อยวันที่ 7 เมษายน 2020 โดย Zoom เวอร์ชั่น 4.6.10 (20033.0407)

รายละเอียด

ความเสี่ยงนี้เกิดจากผู้ไม่หวังดีได้รับ Meeting ID การประชุม หรือค้นหาจากแหล่งสาธารณะหรือรูปการประชุมที่มองเห็น Meeting ID ผู้ไม่หวังดีสามารถทดลองเข้าร่วมการประชุมได้โดยใช้ Meeting ID โดยไม่ต้องรับเชิญ ถ้าผู้สร้างห้องประชุมไม่ทำการใส่รหัสห้องประชุม และก่อกวนด้วยวิธีการต่างๆ เช่นส่งเสียงรบกวนหรือเปิดกล้องเพื่อแสดงร่างกายเปลือย, ส่งภาพอนาจาร, ภาพที่น่าเกลียดหรือคำพูดที่ไม่สุภาพเพื่อทำลายการประชุม

REFERENCE:

- https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows
- https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

2. ช่องโหว่อนุญาตให้แฮกเกอร์ลักลอบเข้ามาเปิดเว็บแคมของผู้ใช้และไมโครโฟนบนเครื่อง MAC โดยไม่ได้รับอนุญาตด้วยการหลอกให้ผู้ใช้เข้าไปเยี่ยมชมเว็บไซต์ที่เป็นอันตราย

ระดับความเสี่ยง

ผู้ไม่หวังดีสามารถแอบมองภาพผ่านกล้องเว็บแคมของผู้ที่แอปพลิเคชัน Zoom บนเครื่อง Mac

สถานะการแก้ไข

ดำเนินการแก้ไขเรียบร้อยวันที่ 2 เมษายน 2020 โดย Zoom เวอร์ชั่น 4.6.9 (19273.0402)

รายละเอียด

Jonathan Leitschuh นักวิจัยความมั่นคงปลอดภัยไซเบอร์ ได้รายงานถึงช่องโหว่ของ Zoom ที่เปิดทางแฮกเกอร์ให้แอบมองภาพผ่านกล้องเว็บแคมของผู้ที่ "เคยติดตั้งแอป" Zoom บนเครื่อง Mac โดยช่องโหว่ใช้เทคนิคสำหรับอำนวยความสะดวกให้ผู้ใช้ ให้สามารถเข้าร่วมการประชุมได้ง่ายๆ เพียงแค่เปิดลิงก์การประชุมเท่านั้น โดยอาศัยการวางเว็บเซิร์ฟเวอร์ไว้ในเครื่องผู้ใช้ ทำให้คนร้ายสามารถดึงให้เหยื่อเข้ามาร่วมการประชุมใดๆ ด้วยการฝังลิงก์เพื่อส่งคำสั่งให้แอป Zoom เข้าร่วมการประชุม โดยค่าเริ่มต้นของแอปจะเปิดกล้องทันทีที่ร่วมประชุม ที่สำคัญคือเว็บเซิร์ฟเวอร์นี้จะยังคงอยู่ในเครื่องผู้ใช้แม้ผู้ใช้จะถอนแอป Zoom ไปแล้วก็ตาม โดยเว็บเซิร์ฟเวอร์นี้รองรับคำสั่งในการดาวน์โหลดแอป Zoom และกลับมาติดตั้งใหม่

REFERENCE:

- https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS
- https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5
- https://www.grahamcluley.com/zoom-mac-flaw-allows-webcams-to-be-hijacked-because-they-wanted-to-save-you-a-click/

3. ZOOM ถูกฟ้องร้องว่าแอบเก็บข้อมูลผู้ใช้และส่งให้ข้อมูลกลับไปหา FACEBOOK

ระดับความเสี่ยง

Zoom ถูกแอบเก็บข้อมูลผู้ใช้งานโดย Facebook SDK และส่งข้อมูลให้ข้อมูลหา Facebook

สถานะการแก้ไข

ดำเนินการแก้ไขเรียบร้อยวันที่ 27 มีนาคม 2020 โดย Zoom

รายละเอียด

Zoom เลิกใช้ Facebook SDK เพราะว่าข้อมูลล็อกอิน Zoom ด้วย Facebook บน iOS ส่งข้อมูลเครื่องผู้ใช้กลับไป Facebook แม้ Zoom จะประกาศเลิกใช้งานไปแล้วโดยตัว Facebook SDK จะเก็บข้อมูลบางส่วนของผู้ใช้ได้แก่ หมายเลขประจำแอป, เวอร์ชั่นของแอป, เครือข่ายที่โทรศัพท์เคลื่อนที่ที่เชื่อมต่ออยู่, หมายเลขประจำเครื่องสำหรับโฆษณา, จำนวนซีพียู, พื้นที่ดิสก์, ขนาดจอ, รุ่นเครื่อง, ภาษาที่ใช้งาน, โซนเวลา, เวอร์ชั่น iOS, และหมายเลขไอพี ทำให้ทาง Zoom ตัดสินใจเลิกใช้ Facebook SDK สำหรับผู้ใช้ที่ต้องการล็อกอินด้วย Facebook

REFERENCE:

- https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/
- https://www.bloomberg.com/news/articles/2020-03-31/zoom-sued-for-allegedly-illegally-disclosing-personal-data

4. ZOOM ไม่มีการเข้ารหัสแบบ END-TO-END ENCRYPTED (E2EE)

ระดับความเสี่ยง

Zoom ไม่ได้มีการเข้ารหัสระดับ End-to-End encrypted (E2EE) เนื้อหาการประชุมวีดีโอหรือเสียงในขณะ Video Meeting อาจทำให้สามารถสอดแนมการประชุมส่วนตัว

สถานะการแก้ไข

ยังไม่มีสถานะการแก้ไข

รายละเอียด

สำนักข่าว The Intercept เปิดเผยว่า Zoom ไม่ได้มีการเข้ารหัสระดับ End-to-end แต่ Zoom กลับใช้วิธีการเข้ารหัสด้วย TLS หรือวิธีการเข้ารหัสบนเว็บไซต์ตามปกติ ซึ่งเป็นการป้องกันระหว่างทางเท่านั้น (Endpoint-Server) นั่นหมายความว่าตัวเซิร์ฟเวอร์ของ Zoom เองยังสามารถเข้าถึงเนื้อหาการประชุมวีดีโอหรือเสียงได้ ทั้งนี้ Zoom เองก็ออกมายอมรับว่า Zoom ยังไม่ได้ทำการเข้ารหัสแบบ End-to-end ในขณะ Video Meeting การไม่มีการเข้ารหัสแบบ End-to-end ของ Zoom ทำให้สามารถสอดแนมการประชุมส่วนตัวหรืออาจถูกบังคับให้มอบการบันทึกการประชุมให้กับรัฐบาลหรือผู้มีอำนาจบังคับใช้กฎหมายเพื่อตอบสนองต่อคำขอทางกฎหมาย

REFERENCE:

- https://www.theverge.com/2020/3/31/21201234/zoom-end-to-end-encryption-video-chats-meetings
- https://www.techoffside.com/2020/04/zoom-end-to-end-encryption/

5. ความเสี่ยงผู้ใช้ ZOOM อาจพบบุคคลอื่นที่ไม่รู้จักและสามารถดูข้อมูลที่อยู่, อีเมลและรูปถ่ายจากรายชื่อผู้ติดต่อภายใต้โดเมนอีเมลที่ใช้

ระดับความเสี่ยง

ผู้ใช้ Zoom อาจพบบุคคลอื่นที่ไม่รู้จักและสามารถดูข้อมูลที่อยู่, อีเมลและรูปถ่ายจากรายชื่อผู้ติดต่อภายใต้โดเมนอีเมลที่ใช้

สถานะการแก้ไข

ยังไม่มีสถานะการแก้ไข

รายละเอียด

ปัญหานี้ถูกพบโดยผู้ใช้งาน Zoom หลายคนได้ลงทะเบียนด้วยอีเมลส่วนตัว โดยแอพพลิเคชั่น Zoom ได้ทำการจัดกลุ่มผู้ใช้งานบางคนร่วมกันที่ลงทะเบียนภายใต้โดเมนเดียวกัน นั่นหมายความว่า Zoom ไม่สามารถแยกแยะ Company Email กับ Free Email ออกจากกันได้ในบางกรณี ซึ่งทำให้ Free Email สามารถใช้งานฟีเจอร์ Company Directory ทั้งที่ไม่ควรใช้ได้ และทำให้สามารถเห็นข้อมูลส่วนบุคคล, ที่อยู่, อีเมล, และภาพถ่ายใน “Company Directory” ได้แม้ว่าคนเหล่าเป็นเพื่อนร่วมงานหรือไม่ก็ตาม

REFERENCE:

- https: / / www. theverge. com/ 2020/ 3/ 31/ 21201956/ zoom- leak- user- information- email-addresses-photos-contacts-directory
- https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos

6. ช่องโหว่บน ZOOM สามารถขโมย WINDOWS CREDENTIALS ได้

ระดับความเสี่ยง

แฮกเกอร์สามารถขโมยข้อมูล WINDOWS CREDENTIALS ของผู้ใช้งานโดยการคลิกที่ LINK ที่ส่งผ่านห้องแชทการประชุม

สถานะการแก้ไข

ดำเนินการแก้ไขเรียบร้อยวันที่ 23 มีนาคม 2020 โดย Zoom เวอร์ชั่น 4.6.8 (19178.0323)

รายละเอียด

ช่องโหว่บนฟีเจอร์ในการส่งแชทหากันเองของผู้ที่อยู่ในห้องประชุม โดยปัญหาคือการใช้งาน UNC Path ของ Zoom หมายความว่าถ้าผู้ใช้งาน Zoom ผ่านมาง Windows จะมีการเชื่อมต่อไปยัง SMB โปรโตคอล (เป็นโปรโตคอลสำหรับการแชร์ไฟล์, เครื่องพิมพ์หรือพอร์ตแบบอนุกรมบนเครือข่าย) ซึ่งโดยปกติแล้วจะมีการส่งชื่อล็อกอินและ NTLM Password ออกไปด้วย ทั้งนี้นักวิจัยที่ชื่อ @_g0dmode พบว่าเขาสามารถดักจับ Password ที่ส่งเข้ามาได้เพื่อทำการแคร็ก นอกจากนี้นักวิจัยยังชี้ว่าสามารถใช้วิธีการนี้สามารถใช้รันโปรแกรมที่อยู่ในคอมพิวเตอร์ของผู้ใช้งานได้ด้วย

REFERENCE:

- https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows
- https: / / www. catcyfence. com/ it- security/ it- 360/ zoom- client- leaks- windows- login-credentials/
- https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

7. ZOOM แสดงข้อมูลและรูปโปรไฟล์ที่ถูกปกปิดใน LINKEDIN

ระดับความเสี่ยง

ผู้เข้าร่วมประชุมคนอื่นๆ สามารถเข้าถึงข้อมูลโปรไฟล์ LinkedIn โดยอัตโนมัติโดยไม่ต้องขออนุญาตจากผู้ใช้

สถานะการแก้ไข

ดำเนินการแก้ไขเรียบร้อยวันที่ 2 เมษายน 2020 โดย Zoom เวอร์ชั่น 4.6.9 (19273.0402)

รายละเอียด

บริการฟีเจอร์ของ Zoom ที่ชื่อว่า LinkedIn Sales Navigator เป็นบริการ LinkedIn ที่ใช้สำหรับการตรวจหายอดขายของผู้ใช้เมื่อผู้ใช้เข้าสู่การประชุมผ่านเว็บ ฟีเจอร์นี้จะส่งรายชื่อผู้ใช้และที่อยู่อีเมลไปยังระบบภายในของบริษัท Zoom โดยอัตโนมัติข้อมูลนี้จะส่งไปยังโปรไฟล์ LinkedIn ฟีเจอร์นี้ยังอนุญาตให้ผู้เข้าร่วมประชุมคนอื่นๆ เข้าถึงข้อมูลโปรไฟล์ LinkedIn โดยอัตโนมัติโดยไม่ต้องขออนุญาตจากผู้ใช้ นั่นหมายความว่าหากผู้ใช้เข้าร่วมการประชุม แม้ว่าจะไม่ได้ใช้ชื่อจริงหรือใช้นามฝง ผู้เข้าร่วมประชุมคนอื่น ๆ สามารถรวบรวมข้อมูลเกี่ยวกับชื่อจริง, ที่อยู่, ชื่อบริษัทและตำแหน่งงานได้

REFERENCE:

- https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
- https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

8. นักวิจัยเผย ZOOM ส่งทราฟฟิกวิดีโอคอลผ่านจีน ฝั่ง ZOOM แจงเป็นศูนย์ข้อมูลสำรอง

ระดับความเสี่ยง

ความเสี่ยงอาจเกิดจากการการที่ไม่มีการเข้ารหัสแบบ end-to-end และส่งทราฟฟิกวิดีโอคอลผ่านประเทศจีน ซึ่งทางการประเทศจีนสามารถสั่งให้ Zoom ส่งข้อมูลใด ๆ ก็ตามที่ต้องการได้

สถานะการแก้ไข

ยังไม่มีสถานะการแก้ไข

รายละเอียด

นักวิจัยจาก Citizen Lab ออกรายงานข้อมูลว่าบริการวิดีโอคอล Zoom ได้ส่งข้อมูลการโทรศัพท์จากอเมริกาเหนือผ่านประเทศจีนโดยไม่แจ้งให้ผู้ใช้ทราบก่อน รวมถึงกุญแจเข้ารหัสที่ใช้กับข้อมูลเหล่านั้นด้วย ซึ่งหมายความว่าถ้าทางการประเทศจีนต้องการข้อมูลใดๆ ก็สามารถสั่งให้ Zoom ส่งข้อมูลใด ๆ ก็ตามที่ต้องการได้ ทั้งนี้เกิดขึ้นจาก Zoom จะพยายามเชื่อมต่อกับศูนย์ข้อมูลที่อยู่ใกล้ที่สุดกับบริเวณที่ผู้ใช้ แต่ถ้าหากมีปัญหาไม่สามารถเชื่อมต่อได้ ไคลเอนท์จะเชื่อมต่อที่ศูนย์ข้อมูลสำรองที่สามารถรับปริมาณทราฟฟิกที่สูงสุด ซึ่งอาจจะเชื่อมต่อไปต่อศูนย์ข้อมูลประเทศจีนได้ในกรณีที่ศูนย์ข้อมูลแห่งอื่นๆ ทราฟฟิกเต็มหมดแล้ว

REFERENCE:

- https: / / citizenlab. ca/ 2020/ 04/ move- fast- roll- your- own- crypto- a- quick- look- at- the-confidentiality-of-zoom-meetings/
- https://techcrunch.com/2020/04/03/zoom-calls-routed-china/