

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- Financial Damage
- Reputation Damage
- Non-compliance
- Privacy Violation

ผลกระทบต่อระบบ

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Google ออก Security Patch แก้ไขช่องโหว่ในระบบปฏิบัติการ Android หลายรายการ รวมถึงช่องโหว่ Zero-day ใน Qualcomm Graphics (CVE-2026-21385)

วันที่แจ้งเตือน 4 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Google ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในระบบ Android หลายรายการ รวมถึงช่องโหว่ Zero-day ใน Qualcomm Graphics (ช่องโหว่ประเภท Buffer Over-read ทำให้เกิด Memory Corruption (CVE-2026-21385)) ซึ่งถูกนำไปใช้โจมตีจริง

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดต Security Patch ของระบบปฏิบัติการ Android ในอุปกรณ์เคลื่อนที่ที่มีการใช้งานตามที่คุณผลิตให้คำแนะนำ จำกัดการติดตั้งแอปพลิเคชันจากแหล่งที่น่าเชื่อถือหรือบริษัทจัดเตรียมเท่านั้น และกำหนดนโยบายควบคุมการใช้งานแอปพลิเคชันบนอุปกรณ์ของบริษัท และเฝ้าระวัง ตรวจสอบ Log และกิจกรรมที่ผิดปกติบนอุปกรณ์ รวมทั้งทบทวนการดำเนินการมาตรการ Cybersecurity ให้มีประสิทธิภาพอย่างสม่ำเสมอ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- <https://www.bleepingcomputer.com/news/security/google-patches-android-zero-day-actively-exploited-in-attacks/>
- <https://source.android.com/docs/security/bulletin/2026/2026-03-01>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-21385>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ