แจ้งเตือน : ช่องโหว่

High

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ Zero Day ของผลิตภัณฑ์ Samsung Android Devices (CVE-2025-21043)

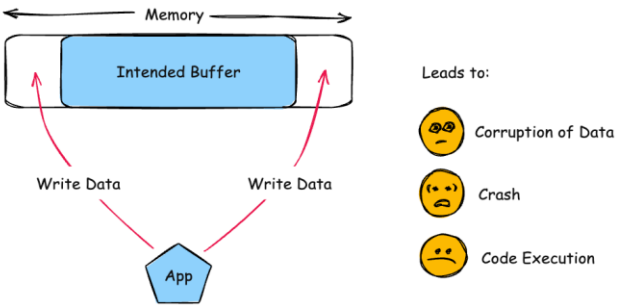
วันที่แจ้งเตือน 19 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีช่องโหว่ Zero Day ที่มีผลกระทบสูงของผลิตภัณฑ์ Samsung Mobile Devices (CVE-2025-21043) ซึ่งผู้ไม่หวังดีมีการใช้ช่องโหว่นี้ในการโจมตีแล้ว โดยมีรายละเอียดดังตาราง

Severity/ CVE ID	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
High: 8.8 CVE-2025-21043	อุปกรณ์ Samsung ที่ใช้งานระบบปฏิบัติการ Android เวอร์ชัน 13, 14, 15, 16	เป็นช่องโหว่ out-of-bounds write* ในไลบรารี libimagecodec.quram.so ซึ่งเป็นไลบรารี ที่ใช้สำหรับการประมวลผลไฟล์รูปภาพ (รองรับไฟล์รูปภาพหลายรูปแบบ) ที่พัฒนาโดย Quramsoft	ผู้โจมตีสามารถรันโค้ดอันตรายบนอุปกรณ์ที่มีช่องโหว่ได้จากระยะไกลได้โดยไม่จำเป็นต้องยืนยันตัวตน ส่งผลให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูลสำคัญ การขโมยข้อมูล (Data theft) หรือ การแก้ไขหรือดัดแปลงข้อมูล (Data manipulation) โดยไม่ได้รับอนุญาต รวมถึงทำความเสียหายแก่ระบบได้
แนวทางการป้องกัน: ผู้ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบ ควรพิจารณาดำเนินการอัปเดตเป็นเวอร์ชันล่าสุด เพื่อป้องกันความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่			

* ช่องโหว่ out-of-bounds เป็นช่องโหว่ที่เกิดจากการเขียนข้อมูลลงในหน่วยความจำที่อยู่นอกขอบเขตของบัฟเฟอร์
(บัฟเฟอร์ คือ หน่วยความจำชั่วคราวใน RAM ใช้สำหรับจัดเก็บข้อมูลระหว่างการส่งต่อหรือประมวลผล เพื่อแก้ปัญหาความแตกต่างของความเร็วในการทำงานของอุปกรณ์ต่าง ๆ ทำให้การไหลของข้อมูลราบรื่นขึ้น และช่วยป้องกันการสูญหายของข้อมูล)



ที่มา: https://cwe.mitre.org/data/definitions/787.html

กรณีหน่วยงานได้อนุญาตให้ผู้ปฏิบัติงานใช้ผลิตภัณฑ์ดังกล่าวเป็น BYOD ควรสื่อสารและพิจารณาอัปเดตระบบปฏิบัติการดังกล่าว เพื่อลดความเสี่ยงของช่องโหว่ที่อาจถูกนำมาใช้และอาจกระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูลสำคัญขององค์กรและลูกค้าได้

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 18 ก.ย. 2568
2) https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-091
3) https://nvd.nist.gov/vuln/detail/CVE-2025-21043