

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

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



ThaiCERT แจ้งเตือนช่องโหว่ความรุนแรงระดับสูง ใน Docker (CVE-2026-34040)

วันที่แจ้งเตือน 17 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณีช่องโหว่ของผลิตภัณฑ์ Docker (CVE-2026-34040) ซึ่งเป็นแพลตฟอร์มใช้สร้างและจัดการ container สำหรับพัฒนาและรันแอปพลิเคชัน เพื่อทำ Authorization Bypass และควบคุมระบบได้

Package	Affected versions	Patched versions	รายละเอียดช่องโหว่
Docker Engine	< 29.3.1	29.3.1	ผู้โจมตีสามารถใช้คำสั่ง API ที่สร้างขึ้นเป็นพิเศษ เพื่อให้ Docker daemon ส่งต่อคำขอ (โดยไม่มีเนื้อหา (Body) ของคำขอนั้นแนบไปด้วย) ไปยังปลั๊กอินตรวจสอบสิทธิ์ (Authorization Plugins: AuthZ) ส่งผลให้ผู้ไม่หวังดีสามารถข้ามผ่านปลั๊กอินตรวจสอบสิทธิ์ได้ ข้อสังเกต: ส่งผลกระทบต่อกรณีที่มีการเปิดใช้ Authorization Plugin (AuthZ) เท่านั้น

แนวทางการป้องกันหรือแก้ไข (Prevention/Mitigation):

- อัปเดต Docker เป็นเวอร์ชัน 29.3.1 หรือใหม่กว่า
- ตรวจสอบและจำกัดการใช้งาน Authorization Plugin ให้เหมาะสม
- จำกัดการเข้าถึง Docker daemon ไม่ให้เปิดสู่สาธารณะ
- ใช้ firewall หรือ network policy เพื่อควบคุมการเข้าถึง
- ตรวจสอบสิทธิ์ของ container และหลีกเลี่ยงการใช้งาน privileged container โดยไม่จำเป็น

แนวทางลดความเสี่ยงกรณียังไม่สามารถอัปเดตได้

- จำกัดการเข้าถึง Docker daemon เฉพาะเครือข่ายภายใน
- ตรวจสอบและจำกัดสิทธิ์ของผู้ใช้งานในระบบ
- เฝ้าระวังการใช้งาน container ที่มีสิทธิ์สูง

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

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 17 เม.ย. 2569
- <https://github.com/moby/moby/security/advisories/GHSA-x744-4wpc-v9h2?>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-34040?>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ