แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือน Docker และ Citrix ออก Security Patch แก้ไขช่องโหว่ระดับร้ายแรง ในผลิตภัณฑ์ Docker Desktop for Windows และ NetScaler ADC/Gateway

**วันที่แจ้งเตือน 3 กันยายน 2568**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ พบว่า Docker และ Citrix ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง ดังนี้

(1) Docker ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-9074) ที่ถูกค้นพบใน Docker Desktop for Windows โดยเป็นช่องโหว่ประเภท Server-Side Request Forgery (SSRF) ซึ่งเปิดโอกาสให้ผู้โจมตีสามารถเข้าถึงไฟล์ของผู้ใช้บนเครื่องโฮสต์ได้โดยไม่ได้รับอนุญาต ช่องโหว่นี้ส่งผลกระทบต่อ Docker Desktop for Windows เวอร์ชัน 4.44.2 และเวอร์ชันก่อนหน้า เพื่อป้องกันความเสี่ยง องค์กรที่ใช้ผลิตภัณฑ์ดังกล่าวควรดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้วโดยทันที เพื่อปิดช่องทางการโจมตีและลดโอกาสในการเข้าถึงข้อมูลโดยมิชอบของผู้โจมตี

(2) Citrix ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-7775) ซึ่งถูกพบในผลิตภัณฑ์ NetScaler ADC และ NetScaler Gateway โดยเป็นช่องโหว่ประเภท Memory Overflow ซึ่งเปิดโอกาสให้ผู้โจมตีสามารถเข้าควบคุมระบบจากระยะไกล (Remote Code Execution - RCE) หรือก่อให้เกิดการหยุดชะงักของบริการ (Denial of Service - DoS) ได้ ช่องโหว่นี้มีผลกระทบต่อหลายเวอร์ชัน ได้แก่ NetScaler ADC และ Gateway ก่อน 14.1-47.48, ก่อน 13.1-59.22, NetScaler ADC 13.1-FIPS/NDcPP ก่อน 13.1-37.241 และ NetScaler ADC 12.1-FIPS/NDcPP ก่อน 12.1-55.330 เพื่อความปลอดภัย องค์กรที่ใช้งานผลิตภัณฑ์ดังกล่าว ควรอัปเดตเป็นเวอร์ชันล่าสุดทันที และสำหรับเวอร์ชันที่สิ้นสุดการสนับสนุนแล้ว (EOL) เช่น 12.1 และ 13.0 แนะนำให้เปลี่ยนไปใช้เวอร์ชันที่ยังได้รับการสนับสนุนโดยด่วน เพื่อลดความเสี่ยงจากการถูกโจมตี

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


**ข้อมูลอ้างอิง**

1. Docker
   1.1 https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-085
   1.2 https://nvd.nist.gov/vuln/detail/CVE-2025-9074
2. Citrix
   2.1 https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-086/
   2.2 https://nvd.nist.gov/vuln/detail/CVE-2025-7775