แจ้งเตือน : ช่องโหว่

Critical

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ Apache Tomcat (CVE-2025-24813)

วันที่แจ้งเตือน 27 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ Apache Tomcat (CVE-2025-24813) โดยช่องโหว่ดังกล่าวเกิดจากการจัดการ HTTP PUT Request ที่ไม่เหมาะสม อาจนำไปสู่การถูกโจมตีในรูปแบบ Remote Code Execution (RCE), การเข้าถึงและเปิดเผยข้อมูลที่มีความอ่อนไหว หรือการเพิ่มเนื้อหาที่เป็นอันตรายลงในไฟล์ที่อัปโหลด หากมีการเปิดใช้งาน Default Servlet ให้มีสิทธิสามารถเขียนไฟล์ได้ (ค่าเริ่มต้น:ปิดใช้งาน)

Apache ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด

Product Name	Affected Version	Solution
Apache Tomcat	11.0.0-M1 to 11.0.2	Upgrade to 11.0.3 or later
	10.1.0-M1 to 10.1.34	Upgrade to 10.1.35 or later
	9.0.0.M1 to 9.0.98	Upgrade to 9.0.99 or later

ThaiCERT แนะนำให้หน่วยงานควรเฝ้าระวังและตรวจสอบช่องโหว่ภายในบริษัท และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของบริษัทเป็นประจำสม่ำเสมอ

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 27 มี.ค. 2568
2) https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
3) https://nvd.nist.gov/vuln/detail/CVE-2025-24813
4) https://nsfocusglobal.com/apache-tomcat-remote-code-execution-vulnerability-cve-2025-24813/