เอกสารการแจ้งเตือนกรณีช่องโหว่ใน Apache Tomcat

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีช่องโหว่ร้ายแรงใน Apache Tomcat

Apache ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ ระดับ Critical ที่หมายเลข CVE-2025-24813 มีคะแนน CVSS 9.8 ส่งผลกระทบต่อ Apache Tomcat ซึ่งเป็นช่องโหว่ Path Equivalence ผ่าน 'file.Name' (จุดภายในชื่อไฟล์) ที่อาจนำไปสู่ Remote Code Execution (RCE), การเปิดเผยข้อมูลหรือการเพิ่มเนื้อหาที่เป็นอันตรายลงในไฟล์ที่อัปโหลด หากมีการเปิดใช้งาน Default Servlet ที่สามารถเขียนไฟล์ได้ แนะนำให้ผู้ใช้ Apache Tomcat ควรทำการอัปเดตทันทีเพื่อลดความเสี่ยงจากช่องโหว่นี้ [1]

Version ที่ได้รับผลกระทบมีดังต่อไปนี้ [2]

- Version 11.0.0-M1 ถึง 11.0.2 ควรอัปเดตเป็น Version 11.0.3
- Version 10.1.0-M1 ถึง 10.1.34 ควรอัปเดตเป็น Version 10.1.35
- Version 9.0.0.M1 ถึง 9.0.98 ควรอัปเดตเป็น Version 9.0.99

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2025-24813
2. https://nsfocusglobal.com/apache-tomcat-remote-code-execution-vulnerability-cve-2025-24813/