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 SAP S/4HANA (CVE-2025-42957)

วันที่แจ้งเตือน 11 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ SAP S/4HANA (CVE-2025-42957) โดยมีรายละเอียดดังตาราง

Severity/ CVE ID	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
Critical: 9.9 CVE-2025-42957	• SAP S/4HANA (Private Cloud และ On-Premise) ที่ใช้ Enterprise Management component (S4CORE) Version 102, 103, 104, 105, 106, 107 และ 108 • Landscape Transformation (Analysis Platform), DMIS versions 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 • Business One (SLD), version B1_ON_HANA 10.0 and SAP-M-BO 10.0 • NetWeaver Application Server ABAP (BIC Document), versions S4COREOP 104, 105, 106, 107, 108, SEM-BW 600, 602, 603, 604, 605, 634, 736, 746, 747, 748	เป็นช่องโหว่ Code Injection ส่งผลให้ผู้ไม่หวังดีที่ครอบครองสิทธิระดับผู้ใช้งานทั่วไป (User privileges) อาศัยช่องโหว่ดังกล่าว เพื่อแทรกคำสั่งและรันโค้ดบนระบบ และเข้าควบคุมระบบภายในบริษัททั้งหมดได้	• การขโมยข้อมูล (Data theft) • การแก้ไขหรือดัดแปลงข้อมูล (Data manipulation) • การยกระดับสิทธิ (Privilege escalation) • การขโมยข้อมูลผู้ใช้งานระบบ (Credential theft) • การรบกวน หรือ ทำให้ระบบงานหยุดชะงักด้วยมัลแวร์ แรนซัมแวร์ หรือวิธีการอื่น ๆ

แนวทางการป้องกัน:

- ติดตั้งแพตช์: หากยังไม่สามารถดำเนินการ ควรติดตั้งอัปเดตความปลอดภัยของ SAP ประจำเดือนสิงหาคม 2025 (Notes 3627998 และ 3633838)
- ตรวจสอบความเสี่ยง: พิจารณาใช้งาน SAP UCON เพื่อจำกัดการใช้งาน RFC และทบทวน จำกัดสิทธิการเข้าถึง object S_DMIS activity 02
- ตรวจสอบบันทึกเหตุการณ์ (Logs): ให้ความสำคัญกรณีมีการเรียกใช้งาน RFC ที่ผิดปกติ การสร้างผู้ใช้ผู้ดูแลระบบใหม่ หรือการเปลี่ยนแปลงโค้ด ABAP และดำเนินการปิดความเสี่ยง
- เสริมความแข็งแกร่งในการป้องกัน: ตรวจสอบให้มั่นใจว่ามีการแบ่งแยกเครือข่าย (Segmentation) การสำรองข้อมูล (Backups) และการติดตามเฝ้าระวังที่เฉพาะเจาะจงสำหรับ SAP

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 11 ก.ย. 2568
2) https://nvd.nist.gov/vuln/detail/CVE-2025-42957
3) https://securitybridge.com/blog/critical-sap-s-4hana-code-injection-vulnerability-cve-2025-42957/
4) https://www.bleepingcomputer.com/news/security/critical-sap-s-4hana-vulnerability-now-exploited-in-attacks/