

แจ้งเตือนช่องโหว่ SalesBleed ใน Salesforce Agentforce

วันที่แจ้งเตือน 7 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ พบรายงานเกี่ยวกับช่องโหว่ SalesBleed ที่กระทุการใช้งาน AI Agent ใน Salesforce Agentforce ซึ่งอาจทำให้ข้อมูลภายในองค์กรรั่วไหล โดยที่ผู้ใช้ไม่ต้องคลิกลิงก์หรือเปิดไฟล์อันตรายแต่อย่างใด (Zero-Click Data Exfiltration) ดังนี้

ช่องโหว่	ผลกระทบ
- ช่องโหว่ประเภท Prompt Injection โดยผู้ไม่หวังดีจะแฝงคำสั่งอันตรายในข้อมูลที่ส่งเข้าระบบ เช่น Salesforce Web-to-Lead Form และหลอกให้ AI นำคำสั่งดังกล่าวไปประมวลผลเสมือนเป็นคำสั่งที่ได้รับอนุญาต - เมื่อข้อมูลถูกบันทึกเข้าสู่ระบบ และผู้ใช้งานเรียก Agentforce เพื่อช่วยวิเคราะห์ข้อมูล AI อาจดำเนินการตามคำสั่งอันตรายดังกล่าว เช่น การค้นหา เข้าถึง หรือส่งข้อมูลออกไปภายนอก เป็นต้น - พบความเสี่ยงในกรณีที่ Agentforce เชื่อมต่อกับบริการอื่น เช่น Slack ซึ่งอาจถูกนำไปใช้เป็นช่องทางส่ง Phishing หรือดำเนินการแทนผู้ใช้งานโดยไม่ได้รับอนุญาต หากมีการกำหนดสิทธิ์ไม่เหมาะสม	- ข้อมูลใน Salesforce CRM ถูกเข้าถึงหรือส่งออกโดยไม่ได้รับอนุญาต - ข้อมูลลูกค้า และข้อมูลธุรกิจสำคัญอาจรั่วไหล - AI Agent อาจทำงานเกินขอบเขตที่ตั้งใจไว้ - ระบบที่เชื่อมต่อ เช่น Slack อาจถูกใช้เป็นช่องทางโจมตีภายในองค์กร ระบบที่ควรตรวจสอบ: หน่วยงานที่ใช้งาน Salesforce Agentforce ควรตรวจสอบในกรณีดังต่อไปนี้ - ระบบที่เปิดใช้งาน Salesforce Agentforce - ระบบที่ใช้งาน Web-to-Lead หรือรับข้อมูลจากบุคคลภายนอก - ระบบที่ให้ Agentforce เข้าถึงข้อมูลสำคัญภายใน Salesforce CRM - ระบบที่เชื่อมต่อ Agentforce กับ Slack หรือบริการภายนอกอื่น - ระบบที่กำหนดให้ AI Agent สามารถดำเนินการแทนผู้ใช้งานได้

แนวทางป้องกัน:

- ใช้หลัก Least Privilege จำกัดสิทธิ Agentforce เท่าที่จำเป็น
- ตรวจสอบ Trusted URLs และการเชื่อมต่อกับระบบภายนอก
- กลั่นกรองแหล่งข้อมูลจากภายนอกก่อนส่งให้ AI ประมวลผล
- ติดตาม Log และกิจกรรมของ Agentforce อย่างสม่ำเสมอ
- ควบคุมสิทธิการเชื่อมต่อกับ Slack และบริการอื่น
- ติดตามคำแนะนำด้านความปลอดภัยล่าสุดจาก Salesforce และปรับปรุงการตั้งค่าอย่างต่อเนื่อง

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 ต.ค. 2569

2. <https://www.securityweek.com/salesbleed-flaws-in-salesforce-agentforce-enabled-zero-click-data-exfiltration/>

3. <https://labs.zenity.io/post/salesbleed-0-click-data-exfiltration-on-agentforce>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT

Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์