

วันที่ 14 ตุลาคม 2569

Anthropic เปิดตัวเครื่องมือ AI สแกนหาช่องโหว่ฟรีสำหรับโครงการโอเพนซอร์ส



เมื่อวันพฤหัสบดีที่ผ่านมา Anthropic ได้เปิดตัว OSS Scanner เครื่องมือสแกนหาช่องโหว่ด้านความปลอดภัยที่ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) เพื่อช่วยยกระดับความปลอดภัยให้กับโครงการซอฟต์แวร์โอเพนซอร์ส โดยเปิดให้ผู้ดูแลโครงการที่สนใจสมัครเข้าร่วมใช้งานได้โดยสมัครใจ

Anthropic ระบุว่าบริการนี้เปิดให้เข้าร่วมโดยสมัครใจ และพัฒนาขึ้นจากประสบการณ์ในการใช้ Claude ค้นหาช่องโหว่ด้านความปลอดภัยภายใต้โครงการ Project Glasswing โดยโครงการที่เข้าร่วมจะได้รับการตรวจสอบความปลอดภัยอย่างละเอียดเป็นระยะ ด้วย AI รุ่นที่มีประสิทธิภาพสูงสุดของเรา โดยไม่มีค่าใช้จ่าย

Anthropic ยังอธิบายว่า ผลการตรวจสอบจากเครื่องมือดังกล่าวจะถูกสร้างขึ้นโดย AI ทั้งหมด โดยไม่จำเป็นต้องผ่านการตรวจสอบหรือคัดกรองจากมนุษย์ก่อนส่งรายงาน ซึ่งช่วยให้สามารถตรวจสอบช่องโหว่ได้รวดเร็วและบ่อยครั้งมากขึ้น ทั้งนี้ รายงานจะถูกสร้างขึ้นด้วย AI รุ่นที่มีประสิทธิภาพสูงสุดของบริษัท รวมถึง Claude Mythos

บริษัทระบุว่า การคัดเลือกโครงการที่จะเข้าร่วมบริการคาดว่าจะใช้หลักเกณฑ์ที่คล้ายกับโครงการ OSS-Fuzz ของ Google แต่อาจมีการปรับเปลี่ยนแนวทางในอนาคต โดยแนะนำให้ผู้ดูแลโครงการเขียนคำอธิบายสั้นๆ เกี่ยวกับความสำคัญของโครงการ หากยังไม่สามารถเห็นความสำคัญได้อย่างชัดเจนจากข้อมูลที่มีอยู่

ผู้ดูแลหลักของโครงการสามารถสมัครเข้าร่วมได้โดยส่ง Pull Request ไปยัง GitHub Repository ของ OSS Scanner พร้อมแนบไฟล์กำหนดค่าในรูปแบบ YAML ซึ่งต้องระบุข้อมูลดังต่อไปนี้

- ลิงก์ไปยัง Git Repository ที่ต้องการให้เครื่องมือดึงโค้ดมาตรวจสอบ
- อีเมลของผู้ติดต่อหลักสำหรับรับรายงาน
- ตำแหน่งไฟล์ Dockerfile ภายใน Repository ซึ่งใช้สำหรับเตรียมสภาพแวดล้อม ติดตั้งส่วนประกอบที่จำเป็นทั้งหมด และสร้างโปรเจกต์ให้พร้อมใช้งาน เพื่อให้ AI สามารถตรวจสอบความปลอดภัยได้โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต

Anthropic อธิบายว่าไฟล์ Dockerfile จะใช้สำหรับกำหนดสภาพแวดล้อมที่โครงการทำงาน รวมถึงติดตั้งส่วนประกอบที่จำเป็นทั้งหมด เพื่อให้ AI สามารถตรวจสอบความปลอดภัยได้โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต โดยเราแนะนำให้ตรวจสอบด้วยว่าชุดทดสอบต่างๆ สามารถทำงานได้ตามปกติภายใน Container ที่สร้างขึ้น

นอกจากนี้ ผู้ดูแลโครงการยังสามารถเพิ่มข้อมูลอื่นๆ ลงในไฟล์ YAML ได้ตามต้องการ ดังนี้

- อีเมลเพิ่มเติมของผู้ที่ต้องการให้ได้รับสำเนารายงานทุกฉบับ
- เว็บไซต์หลักของโครงการ
- กุญแจสาธารณะ GPG (GPG Public Key) สำหรับเข้ารหัสอีเมลรายงาน
- ตำแหน่งไฟล์ Threat Model (threat_model.md) ภายใน Repository ซึ่งใช้ระบุขอบเขตของโค้ดที่ต้องการตรวจสอบ ประเภทของช่องโหว่ หรือรูปแบบรายงานที่ต้องการ
- สามารถเลือกไม่รับรายงานช่องโหว่ได้ โดยกำหนดค่า "disabled: true"

ณ เวลาที่รายงานข่าว มีการส่ง Pull Request เพื่อสมัครเข้าร่วมโครงการแล้วทั้งหมด 116 รายการ โดย Anthropic ระบุว่าแตกต่างจากโครงการรายงานช่องโหว่ทั่วไป บริษัทไม่มีแผนที่จะกำหนดระยะเวลาเปิดเผยข้อมูลช่องโหว่ภายใน 90 วัน เนื่องจากผลการตรวจสอบที่สร้างโดย AI อาจมีการแจ้งเตือนผิดพลาด (False Positive) หรือระบุหาพบช่องโหว่ทั้งที่ไม่ได้มีอยู่จริง

Anthropic อธิบายเพิ่มเติมว่าหากในภายหลังเรานำรายงานใดมาตรวจสอบและยืนยันโดยมนุษย์ผ่านโครงการ Coordinated Vulnerability Disclosure (CVD) ที่มีอยู่ เราอาจเปิดเผยข้อมูลช่องโหว่นั้นตามนโยบาย CVD โดยเริ่มนับระยะเวลา 90 วันตั้งแต่วันที่ผู้ดูแลโครงการได้รับแจ้งว่ารายงานดังกล่าวผ่านการตรวจสอบและยืนยันจากมนุษย์แล้ว

เมื่อเรามีความมั่นใจในประสิทธิภาพของ OSS Scanner มากขึ้น ในอนาคตเราอาจกำหนดระยะเวลาสำหรับการเปิดเผยข้อมูลช่องโหว่บางรายการที่มีระดับความรุนแรงสูง

บริษัทด้าน AI แห่งนี้เปิดเผยว่า ที่ผ่านมาได้ค้นพบช่องโหว่ที่อาจเกิดขึ้นมากกว่า 29,000 รายการ ในโครงการซอฟต์แวร์สำคัญหลายแห่งทั่วโลก โดยมีการแจ้งข้อมูลช่องโหว่ให้ผู้ดูแลโครงการทราบแล้วมากกว่า 6,000 รายการ และนำไปสู่การเผยแพร่ประกาศแจ้งเตือนด้านความปลอดภัย (Security Advisories) จำนวน 584 ฉบับ ณ วันที่ 2 ตุลาคม 2026

การเปิดตัว OSS Scanner เกิดขึ้นในช่วงเดียวกับที่ Anthropic ประกาศเปิดตัว Critical Infrastructure Defense Program ซึ่งเป็นโครงการที่มุ่งปกป้องระบบโครงสร้างพื้นฐานสำคัญและซอฟต์แวร์โอเพนซอร์ส โดยเป็นส่วนหนึ่งของโครงการ Cyber Mission ของบริษัท

ปัจจุบัน AI กำลังกลายเป็นเครื่องมือที่ช่วยให้ผู้โจมตีสามารถค้นหาและใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยได้ง่ายขึ้น รวมถึงช่วยให้ขั้นตอนต่างๆ ของการโจมตีทางไซเบอร์เป็นไปโดยอัตโนมัติ ส่งผลให้การโจมตีเกิดขึ้นได้รวดเร็วและขยายวงกว้างได้มากกว่าเดิม

ด้วยเหตุนี้ Anthropic จึงต้องการพัฒนาเครื่องมือที่ช่วยให้ฝ่ายป้องกันสามารถรับมือกับภัยคุกคามเหล่านี้ได้อย่างมีประสิทธิภาพมากขึ้น ทั้งการเร่งค้นหาและแก้ไขช่องโหว่ ตลอดจนการศึกษาแนวทางออกแบบระบบและพัฒนาซอฟต์แวร์ให้มีความปลอดภัยตั้งแต่เริ่มต้น

Anthropic กล่าวทิ้งท้ายว่า เราคาดการณ์ว่าภายในอีกสองปีข้างหน้า AI จะเข้ามามีบทบาทสำคัญในการช่วยฝ่ายป้องกันมากขึ้น โดยจะทำให้การค้นหาข้อผิดพลาดก่อนเผยแพร่ซอฟต์แวร์เป็นเรื่องง่ายขึ้น สามารถพัฒนาซอฟต์แวร์ที่มีความปลอดภัยตั้งแต่พื้นฐาน และใช้ AI ช่วยปกป้องระบบจากภัยคุกคามได้อย่างต่อเนื่อง

ข้อมูลอ้างอิง

Oct 9, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/anthropic-launches-free-ai.html>