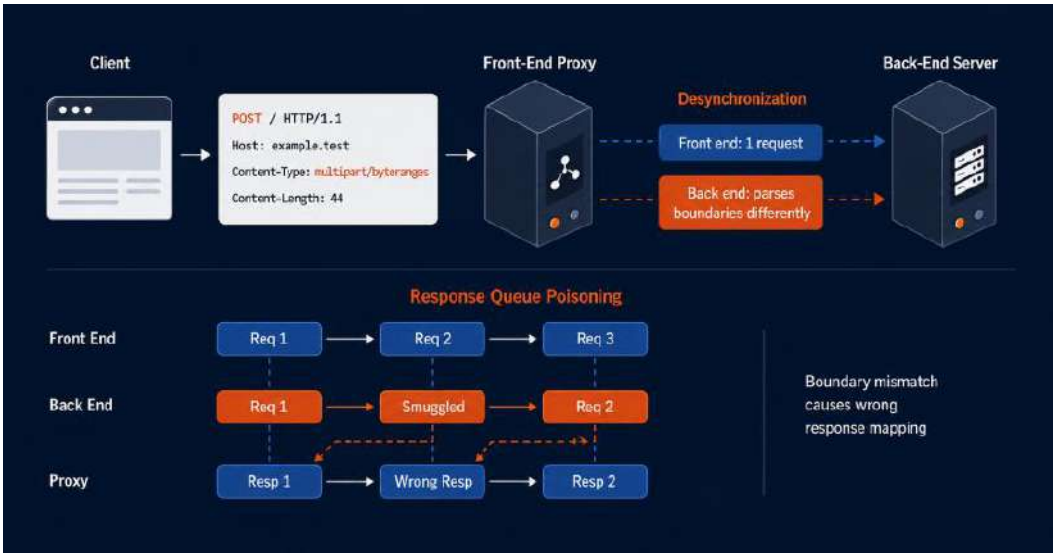
วันที่ 10 สิงหาคม 2569

AI-Assisted HTTP Terminator ค้นพบเทคนิค HTTP Desync รูปแบบใหม่และ Zero-Day ใน Apache



PortSwigger ระบุว่า HTTP Terminator ซึ่งเป็นระบบวิจัยที่ใช้ปัญญาประดิษฐ์ (AI) ช่วยในการค้นหาช่องโหว่ และพัฒนาโดย James Kettle สามารถสร้างและพิสูจน์เทคนิคใหม่สำหรับการโจมตี HTTP Desynchronization ได้ หลังจากทดลองสำรวจรูปแบบการโจมตีที่เป็นไปได้จำนวน 30,000 รูปแบบ

PortSwigger ระบุว่า การค้นหาอีกชุดหนึ่งที่มีมนุษย์เป็นผู้ชี้นำยังสามารถนำไปสู่การค้นพบช่องโหว่ Zero-Day ใน Apache Traffic Server ได้อีกด้วย Kettle กล่าวว่า HTTP Terminator ทดสอบเว็บไซต์จำนวน 30,000 แห่ง ซึ่งได้รับอนุญาตให้สแกนผ่านโครงการ Bug Bounty หรือโครงการเปิดเผยช่องโหว่ และพบเป้าหมายที่มีช่องโหว่ประมาณ 700 แห่ง ก่อนจะเข้าสู่ขั้นตอนตรวจสอบเชิงลึกและการวิจัย RQP

Kettle ระบุว่า ผลการค้นพบดังกล่าวเกี่ยวข้องกับธนาคาร ระบบโครงสร้างพื้นฐานของภาครัฐ ผลิตภัณฑ์ด้านความปลอดภัย และสนามบินแห่งหนึ่ง

งานวิจัยนี้ทำให้พบวิธีใหม่ในการกระตุ้นให้เกิด Desync รูปแบบ Content-Length ที่จับคู่กันสองชั้น และเทคนิคที่เรียกว่า "dangling-byte" ซึ่งออกแบบมาเพื่อทำให้ Response Queue Poisoning (RQP) มีความน่าเชื่อถือมากขึ้น RQP อาจทำให้ระบบ Front End สับสนว่า Response จากฝั่ง Back End ใดเป็นของผู้ใช้คนใด และอาจส่งผลให้ข้อมูลของผู้ใช้อื่นถูกเปิดเผย เช่น Session Cookie หรือ API Key

นักวิจัยยังเปิดเผยแนวคิดการโจมตีที่เรียกว่า Shared-Parser Confusion ซึ่งเป็นแนวคิดการโจมตีในวงกว้างที่ระบบเสนอขึ้นมา แต่ Kettle เป็นผู้ตรวจสอบและยืนยัน Defense ที่ใช้ป้องกันยังคงเหมือนเดิม โดย PortSwigger แนะนำให้หลีกเลี่ยง

การใช้ HTTP/1.1 ในการเชื่อมต่อไปยัง Upstream หากไม่สามารถยกเลิก HTTP/1.1 ได้ ควรกำหนด Allow-list ของ Method ที่อนุญาตในทั้งสองชั้น และจำกัดว่า Method ใดสามารถส่ง Request Body ได้

ในรายงานทางเทคนิค Kettle ระบุว่า เขาป้อน RFC ที่เกี่ยวข้องกับ HTTP และ SMTP จำนวน 138 ฉบับให้กับ HTTP Terminator RFC เหล่านี้ถูกแบ่งออกเป็น Fragment ขนาดเล็กประมาณ 15,000 ส่วน และนำมาใช้เป็นแรงบันดาลใจในการสร้างรูปแบบการโจมตีที่เป็นไปได้จำนวน 30,000 รูปแบบที่ไม่ซ้ำกัน

เทคนิค Content-Type: multipart/byteranges รูปแบบหนึ่งสามารถทำงานได้กับ Server หลายรูปแบบ และพบเว็บไซต์ที่มีช่องโหว่มากกว่า 200 แห่งในชุดทดสอบ ซึ่งรวมถึงธนาคารแห่งหนึ่งในสหรัฐฯ ที่ไม่ได้มีการเปิดเผยชื่อ

จากนั้นระบบวิจัยอัตโนมัติได้ทดสอบแนวคิด 16 รูปแบบเพื่อปรับปรุง RQP โดยมีเพียงเทคนิค dangling-byte ที่ผ่านการประเมิน เทคนิคนี้จะทำให้ Request ที่ถูกแอบส่งเข้ามามีความยาวสั้นกว่าที่ควรหนึ่ง Byte ทำให้ Response จาก Back End ตัวที่สองยังไม่ถูกสร้างขึ้นจนกว่า Request ของเหยื่อจะส่ง Byte ที่ขาดหายไปเข้ามา ส่งผลให้สามารถกำจัด Race Condition ซึ่งเป็นสาเหตุที่ทำให้ RQP ทำงานได้ไม่แน่นอนบนเว็บไซต์จำนวนมาก

ในการค้นหาที่มีมนุษย์เป็นผู้ชี้นำ Request ที่มีรูปแบบผิดปกติทำให้ในท้ายที่สุดพบ Zero-Day ที่เกี่ยวข้องกับ Desynchronization ใน Apache Traffic Server นักวิจัยระบุว่าปัญหานี้ได้รับการแก้ไขแล้ว และถูกติดตามภายใต้หมายเลข CVE-2026-63078

อย่างไรก็ตาม การตรวจสอบของ The Hacker News เมื่อวันที่ 7 สิงหาคม ไม่พบข้อมูลสาธารณะของ CVE-2026-63078 บน CVE.org หรือ NVD และคำแนะนำด้านความปลอดภัยของ Apache ประจำเดือนกรกฎาคม ซึ่งครอบคลุมช่องโหว่จำนวน 34 รายการ ก็ไม่ได้ระบุช่องโหว่นี้ไว้ ทำให้ยังมีช่องว่างในการยืนยันข้อมูลของกรณี Apache เนื่องจากข้อมูลสาธารณะที่มีอยู่ในขณะนี้ยังไม่สามารถระบุได้ว่า CVE-2026-63078 ได้รับการแก้ไขใน Traffic Server รุ่นใด

Kettle ระบุว่า Shared-Parser Confusion เกิดขึ้นเมื่อ HTTP Terminator สังเกตเห็นว่า กฎที่ใช้ประมวลผล Response อาจถูกนำไปใช้กับ Request อย่างไม่ถูกต้อง เมื่อ Server นำ Logic สำหรับการ Parse ข้อมูลกลับมาใช้ร่วมกัน ระบบเป็นผู้เสนอแนวคิดนี้ขึ้นมา แต่ Kettle ซึ่งเป็นผู้อำนวยการฝ่ายวิจัยของ PortSwigger เป็นผู้ตรวจสอบและขยายแนวคิดดังกล่าวให้ชัดเจนขึ้น โดยเขากล่าวว่า "Neither of us would have discovered it alone."

ความแตกต่างดังกล่าวแสดงให้เห็นขอบเขตของความสามารถในการทำงานด้วยตัวเองของระบบในการวิจัยครั้งนี้ ระบบสามารถสร้างและพิสูจน์เทคนิคหลายรูปแบบได้โดยไม่ต้องมีมนุษย์เป็นผู้ค้นพบโดยตรง ขณะที่ Zero-Day ใน Apache และ Shared-Parser Confusion ยังคงต้องอาศัยการเข้ามาตรวจสอบของ Kettle

PortSwigger เปิดซอร์ส HTTP Terminator ให้สาธารณะใช้งานแล้ว อย่างไรก็ตาม งานวิจัยไม่ได้ระบุว่าใช้โมเดลหรือเวอร์ชันใดโดยเฉพาะในการค้นพบแต่ละรูปแบบแบบอัตโนมัติ ส่วน Implementation ที่เผยแพร่ออกมาใช้ Claude สำหรับการดึงข้อมูลจากเอกสารและสร้าง Test Case ขณะที่ขั้นตอน Investigator จำเป็นต้องใช้ Claude Code

นอกจากนี้ นักวิจัยที่อยู่เบื้องหลังการโจมตี Desync ที่ใช้ CRLF ยังได้เผยแพร่เครื่องมือสาธารณะสำหรับศึกษาการโจมตีประเภทดังกล่าว เช่น crlf-desyncs และ crlf-powered-desync-scanner

Kettle ยังได้ทดสอบโมเดลรุ่นใหม่แยกต่างหากบน Benchmark สำหรับการค้นพบช่องโหว่เดิมอีกครั้ง และรายงานว่า GPT-5.6 Sol มีอัตราความสำเร็จ 30% เมื่อได้รับเทคนิคต้นแบบเพื่อใช้เป็นแรงบันดาลใจ

ข้อมูลอ้างอิง

Aug 07, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/ai-assisted-http-terminator-finds-novel.html