แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

เพื่อเฝ้าระวังผู้ไม่หวังดีใช้เทคนิค HTTP Desync เข้าถึงและยึด Session หรือบัญชีของผู้ใช้งาน

วันที่แจ้งเตือน 18 สิงหาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานภัยคุกคามทางไซเบอร์ กรณีมีการเปิดเผยเทคนิค HTTP Desynchronization (HTTP Desync) เพื่อเข้าถึงข้อมูลหรือเกิดผลกระทบต่อ Session ของผู้ใช้งาน โดย

การโจมตี	ระบบที่ได้รับผลกระทบ
ผู้ไม่หวังดีใช้เทคนิคการโจมตี HTTP Desync * ซึ่งเกิดจากการที่ผู้ไม่หวังดีสร้าง Request พิเศษเพื่อส่งให้ Front-end (เช่น Reverse Proxy, Load Balancer, CDN, WAF เป็นต้น) และ Back-end Server ดำเนินการต่อ HTTP Request ไม่ตรงกัน ทำให้ระบบประมวลผลผิดพลาด * ค้นพบโดยเครื่องมือ HTTP Terminator ของ PortSwigger ที่อาศัย AI ในการค้นหาเทคนิคโจมตีใหม่ รวมถึงช่องโหว่ Zero-Day ใน Apache Traffic Server (CVE-2026-63078) 	ควรตรวจสอบเป็นพิเศษหากมีลักษณะดังต่อไปนี้: • Web Application ที่อยู่หลัง Reverse Proxy, Load Balancer, CDN หรือ WAF • ระบบที่ใช้ HTTP/1.1 ระหว่าง Front-end และ Back-end • ระบบที่ Front-end และ Back-end ใช้ HTTP Parser แตกต่างกัน อาจทำให้เกิดการตีความ HTTP Request ไม่สอดคล้องกัน • ระบบที่ยอมรับ HTTP Request ที่ไม่เป็นมาตรฐาน • ระบบที่ยอมให้คำขอ HTTP ที่มีข้อมูลในส่วน Request Body หากเป็น Method ที่โดยปกติไม่จำเป็นต้องมี Body เช่น GET, HEAD หรือ OPTION เป็นต้น • ระบบที่ใช้งาน Apache Traffic Server ที่มีช่องโหว่ CVE-2026-63078

แนวทางการป้องกัน:

- พิจารณาใช้ HTTP/2 หรือสูงกว่า สำหรับการเชื่อมต่อระหว่าง Front-end และ Back-end
- ตรวจสอบการตั้งค่าของ Reverse Proxy, Load Balancer, CDN, WAF และ Back-end Server ให้มีการประมวลผล HTTP Request อย่างสอดคล้องกัน โดยเฉพาะ Header ที่เกี่ยวข้องกับการกำหนดขอบเขตของ Request เช่น Content-Length และ Transfer-Encoding เป็นต้น
- กำหนด Allow-list ของ HTTP Method ทั้งใน Front-end และ Back-end โดยอนุญาตเฉพาะ Method ที่จำเป็นต่อการให้บริการ เช่น POST, PUT หรือ PATCH สามารถมี Request Body ได้ ส่วน GET,HEAD และ OPTIONS ไม่ควรอนุญาตให้มี Request Body หากไม่มีความจำเป็น
- ตรวจสอบและอัปเดต Reverse Proxy, Load Balancer, CDN, Web Server และ WAF ให้เป็นเวอร์ชันล่าสุด โดยเฉพาะผลิตภัณฑ์ที่มีประกาศเกี่ยวกับ HTTP Request Smuggling หรือ HTTP Desync
- ตรวจสอบ Access Logs, Reverse Proxy Logs, WAF Logs และ Back-end Server Logs เพื่อค้นหา Request ที่มีลักษณะผิดปกติดังต่อไปนี้
  1) มี Content-Length มากกว่าหนึ่งรายการโดยไม่มีความจำเป็น
  2) มีการใช้ Content-Length และ Transfer-Encoding ร่วมกันในลักษณะที่ทำให้เกิดความคลุมเครือ
  3) มี HTTP Header หรือโครงสร้าง Request ที่ไม่เป็นไปตามมาตรฐาน

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 18 ส.ค. 2569
2. https://portswigger.net/research/can-ai-do-novel-security-research?
3. https://thehackernews.com/2026/08/ai-assisted-http-terminator-finds-novel.html?