วันที่ 5 มิถุนายน 2569

พบช่องโหว่ HTTP/2 Bomb ใหม่ เสี่ยงถูกโจมตี DoS กระทบ NGINX, Apache, IIS, Envoy และ Cloudflare

นักวิจัยด้านความปลอดภัยทางไซเบอร์ได้ค้นพบวิธีโจมตีแบบใหม่ที่จะทำให้เว็บไซต์หรือเซิร์ฟเวอร์หลักๆ ของโลกอย่าง NGINX, Apache HTTPD, Microsoft IIS, Envoy และ Cloudflare Pingora หยุดทำงานหรือล่มได้ ซึ่งวิธีนี้ถูกเรียกว่า **HTTP/2 Bomb** โดยบริษัท Calif ระบุว่า ช่องโหว่นี้มักพบได้ในการตั้งค่ามาตรฐานของเซิร์ฟเวอร์ส่วนใหญ่ และชี้ว่า OpenAI Codex คือผู้ที่ค้นพบเทคนิคนี้จากการนำแนวคิดการโจมตีสองแบบมารวมกัน นั่นคือ "Compression Bomb" และการค้างการเชื่อมต่อในลักษณะของ "Slowloris"

กลไกการโจมตีผ่าน HPACK และ Flow-Control Window

ทาง Calif อธิบายว่า การโจมตีนี้มุ่งไปที่ HPACK ซึ่งเป็นระบบบีบอัดข้อมูลส่วนหัว (Header) ของ HTTP/2 โดยผู้โจมตีจะส่งข้อมูลเพียง 1 ไบต์ผ่านเครือข่าย แต่สามารถบีบบังคับให้เซิร์ฟเวอร์ต้องสร้างพื้นที่เก็บข้อมูลส่วนหัวขึ้นมามากมาย และทำซ้ำแบบนี้ได้หลายพันครั้งในคำขอเดียว

ส่วนการค้างการเชื่อมต่อนั้น จะใช้เทคนิคที่เรียกว่าการคุมการไหลของข้อมูล (Flow-Control Window) ให้เป็นศูนย์ เพื่อไม่ให้เซิร์ฟเวอร์ปล่อยหน่วยความจำที่ถูกจองไว้คืนมาได้

ทำความรู้จัก HPACK และ Slowloris:

- **HPACK:** คืออัลกอริทึมที่ออกแบบมาเพื่อช่วยบีบอัดข้อมูลส่วนหัวใน HTTP/2 ทำให้ขนาดข้อมูลเล็กลงถึง 30% อีกทั้งยังถูกออกแบบมาเพื่อป้องกันการโจมตีแบบ CRIME ที่อาจทำให้ข้อมูลสำคัญอย่างรหัสผ่านหรือคุกกี้รั่วไหลได้
- **Slowloris:** คือการโจมตีที่ทำให้เซิร์ฟเวอร์ทำงานหนักจนรับไม่ไหว ด้วยการเปิดการเชื่อมต่อค้างเอาไว้จำนวนมากเป็นเวลานาน

ความแตกต่างและจุดเด่นของเทคนิคใหม่

ที่น่าสนใจคือ HTTP/2 Bomb นี้ได้แรงบันดาลใจมาจากเทคนิคเก่าๆ ในอดีตมากมาย ทั้ง HPACK Bomb หรือช่องโหว่ CVE-2016-6581 รวมถึงช่องโหว่อื่นๆ ของ Apache ที่เคยเกิดขึ้นในอดีต แต่จุดที่แตกต่างและถือเป็นความสดใหม่ของการโจมตีครั้งนี้

Calif กล่าวว่า การโจมตีแบบเดิมมักจะใส่ข้อมูลขนาดใหญ่ลงไป ทำให้ผู้พัฒนาเซิร์ฟเวอร์เรียนรู้ที่จะกำหนดเพดานขนาดของข้อมูลไว้ แต่เทคนิคของเรากลับตรงกันข้าม เพราะข้อมูลที่ส่งไปนั้นน้อยมากจนแทบไม่มีอะไรให้ถอดรหัส ทำให้ระบบป้องกันที่เน้นเช็คขนาดข้อมูลหลังถอดรหัสไม่ทำงาน

ความรุนแรงและผลกระทบต่อระบบ

จากสถานการณ์จำลอง นักวิจัยระบุว่าแม้แต่คอมพิวเตอร์ตามบ้านที่ใช้อินเทอร์เน็ตความเร็ว 100 Mbps ก็สามารถทำให้เซิร์ฟเวอร์ล่มได้ภายในเวลาไม่กี่วินาที ยิ่งไปกว่านั้น ผู้โจมตีเพียงคนเดียวก็สามารถยึดพื้นที่หน่วยความจำของ Apache HTTPD และ Envoy ไปได้ถึง 32 GB ภายในเวลาแค่ 20 วินาทีเท่านั้น

คำแนะนำและวิธีการป้องกันความเสี่ยง

สำหรับวิธีการป้องกันความเสี่ยง ผู้ดูแลระบบควรดำเนินการดังนี้:

- **สำหรับ NGINX:** ควรอัปเกรดเป็นเวอร์ชัน 1.29.8 หรือใหม่กว่า ซึ่งมีการเพิ่มคำสั่ง max_headers มาให้ หรือหากอัปเกรดไม่ได้ แนะนำให้ปิดการใช้งาน HTTP/2 ด้วยคำสั่ง http2 off;
- **สำหรับ Apache HTTPD:** ปัญหานี้ได้รับการแก้ไขแล้วใน mod_http2 เวอร์ชัน 2.0.41 หากยังไม่ได้อัปเกรด แนะนำให้ปิดการใช้งาน HTTP/2 โดยเปลี่ยนไปใช้โปรโตคอล http/1.1 แทน
- **สำหรับ Microsoft IIS, Envoy และ Cloudflare Pingora:** ณ ปัจจุบันยังไม่มีแพตช์สำหรับแก้ไขช่องโหว่นี้

บทสรุป

สิ่งที่ผู้คนมักมองข้ามคือ การประเมินความเสี่ยงมักจะดูแค่ว่าข้อมูลขยายตัวได้มากแค่ไหน ทั้งที่จริงๆ แล้วมันเป็นเพียงแค่ครึ่งหนึ่งของปัญหาเท่านั้น Calif กล่าวทิ้งท้าย การที่ข้อมูลขยายตัวได้ 70 ต่อ 1 อาจไม่น่ากลัวเลยถ้าหน่วยความจำถูกคืนกลับทันทีที่ทำงานเสร็จ แต่นี่กลายเป็นการโจมตีได้ เพราะ HTTP/2 ยอมให้ฝั่งผู้ใช้ค้างการเชื่อมต่อไว้ได้นานโดยแทบไม่มีต้นทุน ทำให้หน่วยความจำทุกไบต์ที่ถูกจองไว้ยังคงถูกยึดครองอยู่ได้นานเท่าที่ผู้โจมตีต้องการ

ข้อมูลอ้างอิง

Jun 3, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/new-http2-bomb-vulnerability-allows.html