วันที่ 14 กันยายน 2569

ช่องโหว่ Zero-Day ใน Chrome V8 ถูกนำไปใช้โจมตีแล้ว เปิดทางให้ผู้โจมตีรันโค้ดภายใน Sandbox

Google เมื่อวันอังคารที่ผ่านมาได้ออกอัปเดตเพื่อแก้ไขช่องโหว่ด้านความปลอดภัยจำนวน 230 รายการ รวมถึงหนึ่งช่องโหว่ที่กำลังถูกนำไปใช้โจมตีจริงในขณะนี้ ช่องโหว่ดังกล่าวมีระดับความรุนแรงปานกลาง โดยได้รับหมายเลข CVE-2026-87491 (ยังไม่มีการระบุคะแนน CVSS) และถูกระบุว่าเป็นช่องโหว่ Out-of-Bounds ใน V8 ซึ่งเป็นเอนจิน JavaScript และ WebAssembly ของ Chrome

ช่องโหว่ Out-of-Bounds Write ใน V8 ที่พบใน Google Chrome เวอร์ชันก่อน 153.0.8010.36 เปิดโอกาสให้ผู้โจมตีจากระยะไกลสามารถรันโค้ดที่ต้องการภายใน Sandbox ได้ ผ่านหน้า HTML ที่ถูกสร้างขึ้นมาเป็นพิเศษ ระบุในคำอธิบายช่องโหว่บนฐานข้อมูล National Vulnerability Database (NVD) ของ NIST

Jihyeon Jeong นักวิจัยด้านความปลอดภัยจาก Compsec Lab, Seoul National University ได้รับการยกย่องว่าเป็นผู้ค้นพบและรายงานช่องโหว่นี้เมื่อวันที่ 6 สิงหาคม 2569 โดยนักวิจัยได้รับเงินรางวัล Bug Bounty จำนวน 2,500 ดอลลาร์สหรัฐ จากการรายงานช่องโหว่อย่างรับผิดชอบ

Google ระบุว่า บริษัทรับทราบว่ามีการเผยแพร่ Exploit สำหรับ CVE-2026-87491 และกำลังถูกนำไปใช้โจมตีจริง แต่ยังไม่ได้เปิดเผยรายละเอียดเพิ่มเติมเกี่ยวกับวิธีที่ช่องโหว่นี้ถูกนำไปใช้ในการโจมตีจริง หรือผู้ที่อยู่เบื้องหลังการโจมตี การเข้าถึงรายละเอียดของช่องโหว่และลิงก์ที่เกี่ยวข้องอาจถูกจำกัดไว้จนกว่าผู้ใช้งานส่วนใหญ่จะติดตั้งการแก้ไขแล้ว บริษัทเทคโนโลยีดังกล่าวระบุเพิ่มเติม เราจะยังคงจำกัดการเข้าถึงข้อมูลดังกล่าว หากช่องโหว่นี้อยู่ในไลบรารีของบุคคลที่สามซึ่งโครงการอื่นๆ มีการใช้งานร่วมกัน แต่ยังไม่ได้รับการแก้ไข

จากเหตุการณ์ล่าสุดนี้ Google ได้แก้ไขช่องโหว่ Zero-Day ใน Chrome ที่ถูกนำไปใช้โจมตีจริงแล้วทั้งหมด 7 รายการนับตั้งแต่ต้นปี ซึ่งรวมถึง CVE-2026-2441, CVE-2026-3909, CVE-2026-3910, CVE-2026-5281, CVE-2026-11645 และ CVE-2026-85046

นอกจาก CVE-2026-87491 แล้ว อัปเดตล่าสุดยังแก้ไขช่องโหว่ด้านความปลอดภัยระดับวิกฤตอีก 5 รายการในส่วนประกอบ WebGL และ Cast ได้แก่

- CVE-2026-87464 - ช่องโหว่ Use-after-free ใน WebGL
- CVE-2026-87488 - ช่องโหว่ Use-after-free ใน WebGL
- CVE-2026-87438 - ช่องโหว่ Out-of-Bounds Write ใน WebGL
- CVE-2026-87527 - ช่องโหว่ Buffer Overflow ใน WebGL
- CVE-2026-87628 - ช่องโหว่ Use-after-free ใน Cast

Google ระบุว่า บริษัทเป็นผู้รายงานช่องโหว่ 195 รายการจากทั้งหมด 230 รายการที่ได้รับการแก้ไขในการอัปเดตครั้งนี้ โดยหนึ่งในช่องโหว่ระดับสูงประเภท Use-after-free ใน WebPackaging (CVE-2026-87639) ได้รับเครดิตจาก OpenAI Codex Security ช่องโหว่ด้านความปลอดภัยจำนวนมากของเราถูกตรวจพบด้วยเครื่องมืออย่าง AddressSanitizer, MemorySanitizer, UndefinedBehaviorSanitizer, Control Flow Integrity, libFuzzer หรือ AFL

เพื่อความปลอดภัยสูงสุด ผู้ใช้งานควรอัปเดตเบราว์เซอร์ Chrome เป็นเวอร์ชัน 153.0.8010.36/.37 สำหรับ Windows และ Apple macOS และเวอร์ชัน 153.0.8010.36 สำหรับ Linux โดยสามารถตรวจสอบและติดตั้งการอัปเดตล่าสุดได้ที่ More > Help > About Google Chrome จากนั้นเลือก Relaunch เพื่อเริ่มเบราว์เซอร์ใหม่

สำหรับผู้ใช้งานเบราว์เซอร์อื่นที่พัฒนาบน Chromium เช่น Microsoft Edge, Brave, Opera และ Vivaldi ก็ควรติดตั้งการแก้ไขด้านความปลอดภัยดังกล่าวทันทีที่ผู้พัฒนาแต่ละรายเปิดให้อัปเดต

อัปเดต

สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) เมื่อวันที่ 9 กันยายน 2569 ได้เพิ่ม CVE-2026-87491 ลงในรายการ Known Exploited Vulnerabilities (KEV) ซึ่งกำหนดให้หน่วยงานภาครัฐกลางของสหรัฐฯ ในกลุ่ม Federal Civilian Executive Branch (FCEB) ดำเนินการติดตั้งแพตช์เพื่อแก้ไขช่องโหว่นี้ภายในวันที่ 23 กันยายน 2569

ข้อมูลอ้างอิง

Sep 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/09/chrome-v8-zero-day-exploited-in-wild.html