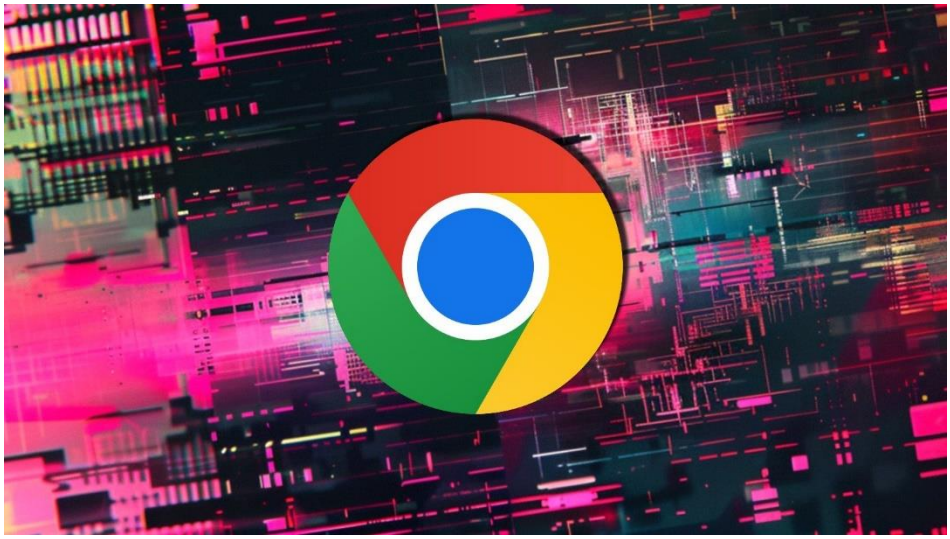
วันที่ 24 กันยายน 2568

Google แก้ไขช่องโหว่ Zero-day บน Chrome ครั้งที่หกที่ถูกใช้โจมตีในปีนี้

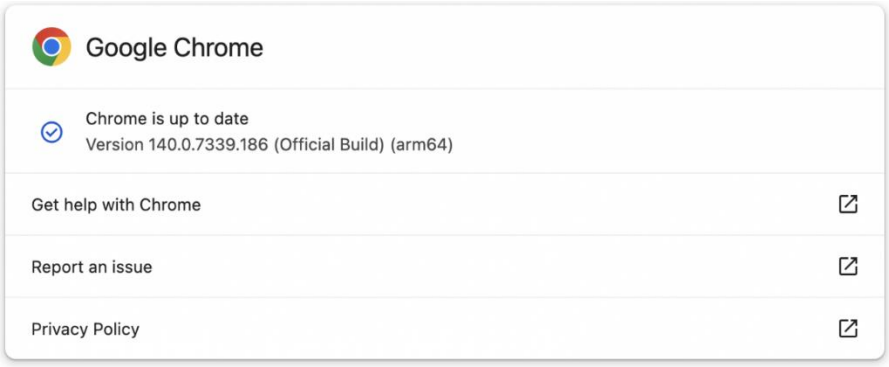


Google ได้ออกอัปเดตความปลอดภัยแบบเร่งด่วนเพื่ออุดช่องโหว่ Zero-day บน Chrome ซึ่งนับเป็นครั้งที่หกแล้วในปีนี้ที่มีการยืนยันว่าถูกนำไปใช้โจมตีจริง แม้ทางบริษัทจะไม่ได้ระบุชัดว่าช่องโหว่นี้ยังคงถูกโจมตีอยู่หรือไม่ แต่ก็ได้เตือนว่ามีโค้ดโจมตีถูกเผยแพร่ออกมาแล้ว ซึ่งโดยทั่วไปถือเป็นสัญญาณว่ามีการโจมตีเกิดขึ้นจริง “Google ทราบแล้วว่ามีการนำช่องโหว่ CVE-2025-10585 ไปใช้โจมตีในโลกจริง” Google ระบุในประกาศความปลอดภัยที่เผยแพร่เมื่อวันพุธที่ผ่านมา

ช่องโหว่ Zero-day ที่มีความรุนแรงสูงนี้ เกิดจากการทำงานผิดพลาดแบบ “type confusion” ใน V8 JavaScript engine ของเบราว์เซอร์ โดยถูกแจ้งมาจากทีม Threat Analysis Group (TAG) ของ Google เมื่อวันอังคาร

ทีม TAG ของ Google มักค้นพบช่องโหว่ Zero-day ที่ถูกใช้โดยกลุ่มที่ได้รับการสนับสนุนจากรัฐบาล เพื่อทำการโจมตีแบบสปายแวร์ที่เจาะจงเป้าหมายบุคคลที่มีความเสี่ยงสูง ไม่ว่าจะเป็นนักการเมืองฝ่ายค้าน นักเคลื่อนไหว หรือผู้สื่อข่าว

ทางบริษัทได้แก้ไขปัญหานี้ในวันถัดมา ด้วยการออกอัปเดต Chrome เวอร์ชัน 140.0.7339.185/.186 สำหรับ Windows/Mac และ 140.0.7339.185 สำหรับ Linux ซึ่งจะทยอยปล่อยให้ผู้ใช้ในช่อง Stable Desktop ภายในไม่กี่สัปดาห์ข้างหน้า ถึงแม้ Chrome จะอัปเดตอัตโนมัติเมื่อมีแพตช์ความปลอดภัยใหม่ แต่ผู้ใช้สามารถเร่งการอัปเดตได้เอง โดยไปที่เมนู Chrome > ความช่วยเหลือ > เกี่ยวกับ Google Chrome จากนั้นรอให้อัปเดตเสร็จ และกดปุ่ม “เริ่มใหม่” เพื่อให้การติดตั้งสมบูรณ์ทันที



แม้ Google จะยืนยันแล้วว่าช่องโหว่ CVE-2025-10585 ถูกใช้ในการโจมตีจริง แต่ยังไม่ได้เปิดเผยรายละเอียดเพิ่มเติมเกี่ยวกับการโจมตีเหล่านั้น “การเข้าถึงรายละเอียดของบั๊กและลิงก์ต่างๆ อาจถูกจำกัดไว้จนกว่าผู้ใช้ส่วนใหญ่จะอัปเดตเป็นเวอร์ชันที่แก้ไขแล้ว” Google กล่าวเสริม “เรายังจะเก็บข้อมูลไว้เป็นความลับ หากบั๊กนี้ไปปรากฏในไลบรารีของบุคคลที่สามที่โครงการอื่นยังใช้อยู่และยังไม่ได้รับการแก้ไข”

นี่เป็นช่องโหว่ Zero-day บน Chrome ที่ถูกใช้โจมตีจริงเป็นครั้งที่หกในปีนี้ หลังจากที่ก่อนหน้านี้มีการแก้ไขไปแล้วห้าครั้งในเดือนมีนาคม พฤษภาคม มิถุนายน และกรกฎาคม

ในเดือนกรกฎาคม Google ได้แก้ไขช่องโหว่ Zero-day (CVE-2025-6558) ที่ทีม TAG ค้นพบ ซึ่งเปิดโอกาสให้แฮ็กเกอร์สามารถหนีออกจาก sandbox ของเบราว์เซอร์ได้

ในเดือนพฤษภาคม Google ก็ออกอัปเดตเร่งด่วนเพื่อแก้ไขช่องโหว่ Zero-day (CVE-2025-4664) ที่ทำให้แฮ็กเกอร์สามารถยึดบัญชีผู้ใช้ และยังแก้ไขช่องโหว่อีกจุดในเดือนมิถุนายน (CVE-2025-5419) ซึ่งเป็นการอ่านและเขียนข้อมูลเกินขอบเขตใน V8 JavaScript engine ที่ค้นพบโดยทีม TAG

ส่วนในเดือนมีนาคม Google ได้อุดช่องโหว่รุนแรง (CVE-2025-2783) ซึ่งถูกค้นพบโดย Kaspersky และถูกใช้ในการโจมตีแบบจารกรรมต่อหน่วยงานรัฐบาลรัสเซียและสื่อมวลชน

ตลอดทั้งปีที่แล้ว Google ยังได้แก้ไขช่องโหว่ Zero-day อีกถึง 10 จุด ที่ถูกนำมาใช้จริงในการแข่งขันแฮ็กอย่าง Pwn2Own หรือถูกนำไปใช้โจมตีในโลกจริงแล้วเช่นกัน

สรุประดับความเสี่ยง

- **ความรุนแรง:** สูง (High Severity)
- **สาเหตุ:** ช่องโหว่แบบ *type confusion* ใน V8 JavaScript engine ของ Chrome
- **ผลกระทบ:** ผู้โจมตีสามารถใช้ช่องโหว่นี้รันโค้ดอันตรายบนเครื่องเหยื่อได้ อาจนำไปสู่การขโมยข้อมูล ยึดบัญชี หรือควบคุมเครื่อง
- **สถานะ:** มีการยืนยันแล้วว่า **ถูกใช้โจมตีจริง (in the wild)**
- **แนวโน้ม:** มักถูกใช้โดยกลุ่มที่ได้รับการสนับสนุนจากรัฐ เพื่อโจมตีเป้าหมายเฉพาะ เช่น นักการเมือง นักเคลื่อนไหว และนักข่าว

แนวทางแก้ไข (สำหรับผู้ใช้ทั่วไปและองค์กร)

1. **อัปเดต Chrome ทันที**
    - ไปที่เมนู ⋮ > **ความช่วยเหลือ > เกี่ยวกับ Google Chrome**
    - รอให้อัปเดตดาวน์โหลดเสร็จ แล้วกด **“เริ่มใหม่ (Relaunch)”**
    - ตรวจสอบให้แน่ใจว่าเวอร์ชันอยู่ที่ **140.0.7339.185/.186** หรือใหม่กว่า
2. **รีบูตเครื่องหลังอัปเดต** เพื่อให้การอัปเดตความปลอดภัยมีผลเต็มที่
3. **ตรวจสอบและอัปเดตเบราว์เซอร์อื่นๆ ที่ใช้ Chromium** เช่น Edge, Opera, Brave เพราะมักใช้เอนจินเดียวกัน
4. **ลดความเสี่ยงชั่วคราว (หากยังอัปเดตไม่ได้)**
    - หลีกเลี่ยงการเข้าเว็บที่ไม่น่าเชื่อถือ
    - ปิดหรือจำกัดการใช้งาน JavaScript ผ่านปลั๊กอินเสริม (เช่น NoScript)
    - ใช้เบราว์เซอร์สำรองที่ได้รับการอัปเดตแล้ว
5. **สำหรับองค์กร**
    - ใช้ **เครื่องมือจัดการแพตช์ (Patch Management)** เพื่อตรวจสอบว่าเครื่องลูกข่ายอัปเดตแล้ว
    - เฝ้าระวัง **การแจ้งเตือนจาก EDR/AV** เกี่ยวกับการรันโค้ดผิดปกติจาก Chrome
    - หลีกเลี่ยงการคลิกลิงก์หรือไฟล์แนบที่ไม่น่าไว้ใจ

ข้อมูลอ้างอิง

Sep 18, 2025, By Sergiu Gatlan

- https://www.bleepingcomputer.com/news/security/google-patches-sixth-chrome-zero-day-exploited-in-attacks-this-year/