วันที่ 3 เมษายน 2569

พบช่องโหว่ Zero-Day ใหม่ใน Chrome หมายเลข CVE-2026-5281 กำลังถูกใช้โจมตี

Google ปล่อยอัปเดตความปลอดภัยสำหรับ Chrome เมื่อวันพฤหัสบดีที่ผ่านมา เพื่อแก้ไขช่องโหว่ทั้งหมด 21 รายการ หนึ่งในนั้นคือช่องโหว่แบบ Zero-Day ที่บริษัทยืนยันแล้วว่ากำลังถูกนำไปใช้โจมตีจริงในโลกออนไลน์

ช่องโหว่นี้คืออะไร และอันตรายแค่ไหน

ช่องโหว่ความรุนแรงสูงที่มีรหัส CVE-2026-5281 เป็นบั๊กประเภท use-after-free ใน Dawnซึ่งเป็นโปรเจกต์โอเพ่นซอร์สที่ Google พัฒนาขึ้นเพื่อรองรับมาตรฐาน WebGPU แบบข้ามแพลตฟอร์ม

บั๊กประเภท use-after-free เกิดขึ้นเมื่อโปรแกรมยังคงอ้างอิงถึงหน่วยความจำที่ถูกปล่อยไปแล้ว ซึ่งผู้โจมตีสามารถใช้ประโยชน์จากจุดนี้เพื่อควบคุมพฤติกรรมของโปรแกรมได้

ตามคำอธิบายในฐานข้อมูลช่องโหว่ของ National Institute of Standards and Technology (NIST) ระบุว่า ช่องโหว่นี้อาจทำให้ผู้โจมตีจากระยะไกลที่สามารถเข้าควบคุม กระบวนการ renderer (ส่วนที่ทำหน้าที่แสดงผลหน้าเว็บ) ได้แล้ว สามารถรันโค้ดใดก็ได้บนเครื่องเหยื่อ เพียงแค่ล่อให้เหยื่อเปิดหน้าเว็บ HTML ที่ถูกสร้างขึ้นมาโดยเฉพาะ

Google รู้แล้ว แต่ยังไม่บอกรายละเอียด

Google ยืนยันว่า "ทราบแล้วว่ามีการใช้ช่องโหว่ CVE-2026-5281 โจมตีจริงในโลกออนไลน์" แต่ยังไม่เปิดเผยรายละเอียดเพิ่มเติม ไม่ว่าจะเป็นวิธีการโจมตีหรือผู้อยู่เบื้องหลัง ซึ่งเป็นแนวปฏิบัติปกติเพื่อป้องกันไม่ให้ผู้ไม่หวังดีรายอื่นนำข้อมูลไปใช้โจมตีเพิ่มเติม ก่อนที่ผู้ใช้ส่วนใหญ่จะได้อัปเดตแพตช์

เหตุการณ์นี้เกิดขึ้นต่อเนื่องจากที่ Google เพิ่งออกแพตช์แก้ไขช่องโหว่ Zero-Day ไปก่อนหน้านี้หลายรายการ ได้แก่ CVE-2026-3909 และ CVE-2026-3910 ซึ่งถูกใช้โจมตีในลักษณะเดียวกัน รวมถึง CVE-2026-2441 ซึ่งเป็นบั๊ก use-after-free ในส่วน CSS ของ Chrome ที่พบในเดือนกุมภาพันธ์

นับตั้งแต่ต้นปีที่ผ่านมา Google ได้ออกแพตช์แก้ไขช่องโหว่ Chrome Zero-Day ที่ถูกใช้โจมตีจริงแล้วทั้งหมด 4 รายการ

เพื่อความปลอดภัย ควรอัปเดต Chrome เป็นเวอร์ชันดังนี้ทันที

- Windows และ macOS: เวอร์ชัน 146.0.7680.177 หรือ 146.0.7680.178
- Linux: เวอร์ชัน 146.0.7680.177

วิธีอัปเดตทำได้โดยไปที่ เมนู (⋮) > Help > About Google Chrome จากนั้นกด Relaunch เพื่อรีสตาร์ตเบราว์เซอร์และติดตั้งอัปเดต

ผู้ที่ใช้เบราว์เซอร์อื่นที่สร้างบนพื้นฐาน Chromium เช่น Microsoft Edge, Brave, Opera และ Vivaldi ก็ควรติดตั้งแพตช์ทันทีเมื่อมีการปล่อยอัปเดตเช่นกัน เนื่องจากช่องโหว่นี้อาจส่งผลกระทบต่อเบราว์เซอร์เหล่านั้นด้วย

ข้อมูลอ้างอิง

Apr 1, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/new-chrome-zero-day-cve-2026-5281-under.html