วันที่ 13 กุมภาพันธ์ 2569

Microsoft ออกแพตช์แก้ไขช่องโหว่ 59 รายการ รวมถึง 6 รายการที่กำลังถูกโจมตีจริงอยู่ในขณะนี้

Microsoft ได้ออกอัปเดตความปลอดภัยเมื่อวันอังคารที่ผ่านมา เพื่อแก้ไขช่องโหว่ทั้งหมดในซอฟต์แวร์ของบริษัท โดยในจำนวนนี้มี 6 ช่องโหว่ที่ถูกนำไปใช้โจมตีจริงแล้วในโลกออนไลน์ จากช่องโหว่ทั้งหมด 59 รายการ มี 5 รายการถูกจัดอยู่ในระดับ Critical (ร้ายแรงมาก), 52 รายการอยู่ในระดับ Important (สำคัญ), และอีก 2 รายการอยู่ในระดับ Moderate (ปานกลาง) และในจำนวนช่องโหว่ที่ได้รับการแก้ไขนั้น 25 รายการเป็นการยกระดับสิทธิ์ (Privilege Escalation), รองลงมาคือการรันโค้ดจากระยะไกล (Remote Code Execution) 12 รายการ, การปลอมแปลง (Spoofing) 7 รายการ, การเปิดเผยข้อมูล (Information Disclosure) 6 รายการ, การข้ามกลไกความปลอดภัย (Security Feature Bypass) 5 รายการ, การทำให้ระบบล่ม (Denial-of-Service) 3 รายการ และ Cross-Site Scripting อีก 1 รายการ

นอกจากนี้ แพตช์ชุดนี้ยังเพิ่มเติมจากช่องโหว่อีก 3 รายการที่ Microsoft ได้แก้ไขไปแล้วก่อนหน้านี้ในเบราว์เซอร์ Microsoft Edge ตั้งแต่การอัปเดต Patch Tuesday เดือนมกราคม 2026 โดยหนึ่งในนั้นเป็นช่องโหว่ระดับ Moderate ที่กระทบต่อ Edge บน Android (CVE-2026-0391, คะแนน CVSS 6.5) ซึ่งอาจเปิดช่องให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถปลอมแปลงข้อมูลผ่านเครือข่ายได้ โดยอาศัยการแสดงผลข้อมูลสำคัญบนหน้าจอที่อาจทำให้ผู้ใช้เข้าใจผิด

ช่องโหว่ที่ถูกจัดว่าเร่งด่วนที่สุดในเดือนนี้ คือ 6 รายการที่กำลังถูกใช้โจมตีจริง ได้แก่

- **CVE-2026-21510 (คะแนน CVSS 8.8)** – ความล้มเหลวของกลไกป้องกันใน Windows Shell ที่เปิดทางให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถข้ามระบบป้องกันผ่านเครือข่ายได้
- **CVE-2026-21513 (คะแนน CVSS 8.8)** – ความล้มเหลวของกลไกป้องกันใน MSHTML Framework ที่เปิดช่องให้ผู้โจมตีที่ไม่ได้รับอนุญาตข้ามระบบป้องกันผ่านเครือข่ายได้
- **CVE-2026-21514 (คะแนน CVSS 7.8)** – การใช้ข้อมูลที่ไม่น่าเชื่อถือในการตัดสินใจด้านความปลอดภัยใน Microsoft Office Word ซึ่งอาจทำให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถข้ามระบบป้องกันได้จากภายในเครื่อง
- **CVE-2026-21519 (คะแนน CVSS 7.8)** – ปัญหา type confusion ใน Desktop Window Manager ที่ทำให้ผู้โจมตีที่มีสิทธิ์อยู่แล้วสามารถยกระดับสิทธิ์ภายในเครื่องได้

- **CVE-2026-21525 (คะแนน CVSS 6.2)** – ปัญหา null pointer dereference ใน Windows Remote Access Connection Manager ซึ่งอาจทำให้ผู้โจมตีที่ไม่ได้รับอนุญาตทำให้ระบบหยุดทำงานจากภายในเครื่องได้
- **CVE-2026-21533 (คะแนน CVSS 7.8)** – การจัดการสิทธิ์ที่ไม่เหมาะสมใน Windows Remote Desktop ซึ่งเปิดช่องให้ผู้โจมตีที่มีสิทธิ์อยู่แล้วสามารถยกระดับสิทธิ์ภายในเครื่องได้

ทีมความปลอดภัยของ Microsoft และ Google Threat Intelligence Group (GTIG) เป็นผู้ค้นพบและรายงานช่องโหว่สามรายการแรก ซึ่งถูกเปิดเผยต่อสาธารณะแล้วในช่วงเวลาที่ออกแพตช์ อย่างไรก็ตาม ขณะนี้ยังไม่มีรายละเอียดว่าช่องโหว่เหล่านี้ถูกนำไปใช้โจมตีอย่างไร และยังไม่ชัดเจนว่าเป็นการโจมตีในแคมเปญเดียวกันหรือไม่

Jack Bicer ผู้อำนวยการฝ่ายวิจัยช่องโหว่ของ Action1 กล่าวว่า CVE-2026-21513 เป็นช่องโหว่แบบข้ามกลไกความปลอดภัยใน Microsoft MSHTML Framework ซึ่งเป็นส่วนประกอบหลักของ Windows และหลายแอปพลิเคชันที่ใช้สำหรับแสดงผลเนื้อหา HTML เขาอธิบายว่า ช่องโหว่นี้เกิดจากความล้มเหลวของกลไกป้องกัน ทำให้ผู้โจมตีสามารถหลีกเลี่ยงหน้าต่างแจ้งเตือนความปลอดภัยได้ เมื่อผู้ใช้เปิดไฟล์ที่เป็นอันตราย ไฟล์ที่ถูกสร้างขึ้นมาอย่างจงใจสามารถข้ามการแจ้งเตือนของ Windows และสั่งให้เกิดการทำงานที่อันตรายได้เพียงคลิกเดียว

Satnam Narang วิศวกรวิจัยอาวุโสจาก Tenable กล่าวว่า CVE-2026-21513 และ CVE-2026-21514 มีลักษณะคล้ายกับ CVE-2026-21510 อย่างมาก โดยความแตกต่างหลักคือ CVE-2026-21513 สามารถโจมตีผ่านไฟล์ HTML ได้ ส่วน CVE-2026-21514 จะโจมตีได้ผ่านไฟล์ Microsoft Office เท่านั้น

สำหรับ CVE-2026-21525 มีความเกี่ยวข้องกับช่องโหว่แบบ zero-day ที่บริการ 0patch ของ ACROS Security ระบุว่าค้นพบในเดือนธันวาคม 2025 ระหว่างการตรวจสอบช่องโหว่อีกตัวในองค์ประกอบเดียวกัน (CVE-2025-59230)

Kev Breen ผู้อำนวยการอาวุโสฝ่ายวิจัยภัยคุกคามไซเบอร์ของ Immersive กล่าวว่า CVE-2026-21519 และ CVE-2026-21533 เป็นช่องโหว่ยกระดับสิทธิ์ภายในเครื่อง หมายความว่าผู้โจมตีต้องเข้าถึงเครื่องเป้าหมายได้ก่อน

การเข้าถึงดังกล่าวอาจเกิดจากไฟล์แนบที่เป็นอันตราย ช่องโหว่รันโค้ดจากระยะไกล หรือการเคลื่อนที่ภายในเครือข่ายจากเครื่องที่ถูกยึดไปแล้ว เมื่อผู้โจมตีอยู่ในเครื่องแล้ว ก็สามารถใช้ช่องโหว่เหล่านี้เพื่อยกระดับสิทธิ์เป็นระดับ SYSTEM ซึ่งเป็นสิทธิ์สูงสุดในระบบ ด้วยสิทธิ์ระดับนี้ ผู้โจมตีอาจปิดการทำงานของเครื่องมือความปลอดภัย ติดตั้งมัลแวร์เพิ่มเติม หรือในกรณีร้ายแรง อาจเข้าถึงข้อมูลลับหรือข้อมูลรับรองตัวตนที่นำไปสู่การยึดครองโดเมนทั้งระบบได้

บริษัทความปลอดภัยไซเบอร์ CrowdStrike ซึ่งเป็นผู้รายงาน CVE-2026-21533 ระบุว่า ยังไม่สามารถชี้ชัดได้ว่าเป็นฝีมือของกลุ่มผู้โจมตีรายใด แต่คาดว่าผู้ที่มีโค้ดโจมตีอยู่ในมืออาจเร่งนำไปใช้หรือขายต่อในเร็วๆ นี้

Adam Meyers หัวหน้าฝ่าย Counter Adversary Operations ของ CrowdStrike กล่าวว่าตัว exploit ของ CVE-2026-21533 มีการแก้ไขค่าในรีจิสทรีของบริการระบบ โดยแทนที่คีย์เดิมด้วยคีย์ที่ผู้โจมตีควบคุม ซึ่งอาจช่วยให้ผู้โจมตีสามารถยกระดับสิทธิ์เพื่อเพิ่มผู้ใช้ใหม่เข้าไปในกลุ่ม Administrator ได้

เหตุการณ์นี้ทำให้ Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐฯ เพิ่มช่องโหว่ทั้ง 6 รายการเข้าไปในรายการ Known Exploited Vulnerabilities (KEV) และกำหนดให้หน่วยงานภาครัฐในสังกัด Federal Civilian Executive Branch (FCEB) ต้องติดตั้งแพตช์แก้ไขภายในวันที่ 3 มีนาคม 2026

พร้อมกันนี้ Microsoft ยังได้เริ่มทยอยอัปเดตใบรับรอง Secure Boot ชุดใหม่ เพื่อทดแทนใบรับรองเดิมที่ออกในปี 2011 ซึ่งจะหมดอายุในปลายเดือนมิถุนายน 2026 โดยใบรับรองใหม่จะถูกติดตั้งผ่านกระบวนการอัปเดต Windows รายเดือนตามปกติ ไม่ต้องดำเนินการเพิ่มเติม

บริษัทระบุว่า หากอุปกรณ์ไม่ได้รับใบรับรอง Secure Boot ชุดใหม่ก่อนที่ใบรับรองปี 2011 จะหมดอายุ เครื่องยังคงใช้งานได้ตามปกติ และซอฟต์แวร์เดิมยังทำงานได้ อย่างไรก็ตาม อุปกรณ์จะเข้าสู่สถานะความปลอดภัยที่ลดลง ซึ่งจำกัดความสามารถในการรับการป้องกันระดับบูตในอนาคต เมื่อมีการค้นพบช่องโหว่ใหม่ในระดับบูต ระบบที่ได้รับผลกระทบจะเสี่ยงมากขึ้น เพราะไม่สามารถติดตั้งมาตรการป้องกันใหม่ได้ และในระยะยาวอาจเกิดปัญหาความเข้ากันได้ เช่น ระบบปฏิบัติการ เฟิร์มแวร์ ฮาร์ดแวร์ หรือซอฟต์แวร์ที่พึ่งพา Secure Boot รุ่นใหม่อาจไม่สามารถทำงานได้

นอกจากนี้ Microsoft ยังประกาศเสริมความแข็งแกร่งด้านความปลอดภัยของ Windows ผ่านสองโครงการ คือ Windows Baseline Security Mode และ User Transparency and Consent ภายใต้กรอบงาน Secure Future Initiative และ Windows Resiliency Initiative

Windows Baseline Security Mode จะทำให้ Windows เปิดใช้งานการป้องกันความถูกต้องของระบบในระหว่างทำงานเป็นค่าเริ่มต้น เพื่อให้เฉพาะแอป บริการ และไดรเวอร์ที่มีลายเซ็นถูกต้องเท่านั้นที่สามารถทำงานได้ ช่วยลดความเสี่ยงจากการแก้ไขหรือดัดแปลงระบบโดยไม่ได้รับอนุญาต

ส่วน User Transparency and Consent มีแนวคิดคล้ายกับกรอบการทำงาน Transparency, Consent, and Control (TCC) ของ Apple macOS โดยจะกำหนดแนวทางที่ชัดเจนในการจัดการการตัดสินใจด้านความปลอดภัย ระบบจะถามผู้ใช้เมื่อแอปพยายามเข้าถึงทรัพยากรสำคัญ เช่น ไฟล์ กล้อง หรือไมโครโฟน หรือเมื่อพยายามติดตั้งซอฟต์แวร์อื่นโดยไม่ได้ตั้งใจ

ข้อมูลอ้างอิง

Feb 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/microsoft-patches-59-vulnerabilities.html