วันที่ 11 มิถุนายน 2569

Microsoft ออกแพตช์แก้ไขช่องโหว่สูงเป็นประวัติการณ์ 206 รายการ รวมถึง Zero-Day 3 รายการ และช่องโหว่ร้ายแรงที่นำไปสู่การรันโค้ดจากระยะไกล

Microsoft ได้ออกอัปเดตความปลอดภัยประจำเดือนเมื่อวันอังคารที่ผ่านมา เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยจำนวนสูงเป็นประวัติการณ์ถึง 206 รายการ ที่ส่งผลกระทบต่อผลิตภัณฑ์ต่างๆ ของบริษัท โดยในจำนวนนี้มีช่องโหว่3 รายการที่ถูกเปิดเผยต่อสาธารณะแล้ว ณ เวลาที่มีการออกแพตช์

จากช่องโหว่ทั้งหมด 206 รายการ มี 39 รายการที่ถูกจัดอยู่ในระดับ Critical และอีก 167รายการอยู่ในระดับ Important โดยแบ่งประเภทได้ดังนี้ ได้แก่ ช่องโหว่ยกระดับสิทธิ์ (Privilege Escalation) 63 รายการ,ช่องโหว่รันโค้ดจากระยะไกล (Remote Code Execution) 56 รายการ, ช่องโหว่เปิดเผยข้อมูล (Information Disclosure) 30 รายการ, ช่องโหว่ปลอมแปลง (Spoofing) 27 รายการ, ช่องโหว่ข้ามกลไกความปลอดภัย (Security Feature Bypass) 20 รายการ, ช่องโหว่ปฏิเสธการให้บริการ (Denial-of-Service) 7 รายการ และช่องโหว่แก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Tampering) อีก 3รายการ

การอัปเดตครั้งนี้ยังรวมถึง CVE ที่ไม่ได้มาจากMicrosoft อีก 2 รายการ ได้แก่ ช่องโหว่ยกระดับสิทธิ์ใน Windows Kernel (CVE-2025-10263) และช่องโหว่ข้ามกลไกความปลอดภัยของUEFI Secure Boot (CVE-2026-8863) นอกจากนี้ ยังมีการรวมการแก้ไขช่องโหว่ด้านความปลอดภัยมากกว่า 350 รายการใน Chromium ซึ่งเป็นโครงการโอเพนซอร์สที่Microsoft Edge ใช้งานอยู่ด้วย

ช่องโหว่ระดับวิกฤตที่อาจนำไปสู่การรันโค้ดจากระยะไกล

ช่องโหว่ที่ถูกจับตามองมากที่สุดคือ CVE-2026-45657 (คะแนน CVSS: 9.8) ซึ่งเป็นช่องโหว่ประเภท Use-After-Freeใน Windows Kernel ที่อาจนำไปสู่การรันโค้ดจากระยะไกลได้ Microsoft ระบุว่า ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นี้ได้

โดยการส่งทราฟฟิกเครือข่ายที่ถูกสร้างขึ้นเป็นพิเศษไปยังระบบWindows ที่มีช่องโหว่ หากการโจมตีสำเร็จ แพ็กเก็ตข้อมูลที่เป็นอันตรายอาจกระตุ้นข้อผิดพลาดในกระบวนการประมวลผลข้อมูล TCP/IPของ Windows Kernel ส่งผลให้ผู้โจมตีสามารถรันโค้ดด้วยสิทธิ์ระดับSYSTEM ได้ โดยไม่จำเป็นต้องเข้าสู่ระบบหรือมีการโต้ตอบจากผู้ใช้งาน

ช่องโหว่สำคัญอื่นๆ ที่น่าสนใจ ได้แก่ · CVE-2026-47291 (คะแนน CVSS: 9.8) - ช่องโหว่ Integer Overflow หรือ Wraparoundใน Windows HTTP.sys ที่เปิดโอกาสให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถรันโค้ดผ่านเครือข่ายได้ · CVE-2026-44815 (คะแนน CVSS: 9.8) - ช่องโหว่ Stack-Based Buffer Overflow ในWindows DHCP Client ที่เปิดโอกาสให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถรันโค้ดผ่านเครือข่ายได้

Alex Vovk ซีอีโอและผู้ร่วมก่อตั้งบริษัท Action1 กล่าวถึง CVE-2026-44815 ว่า ช่องโหว่นี้ไม่จำเป็นต้องใช้ข้อมูลรับรองตัวตน และไม่ต้องอาศัยการกระทำใดๆ จากผู้ใช้ โดยสามารถเปลี่ยนทราฟฟิกเครือข่ายให้กลายเป็นการยึดระ บบได้อย่างสมบูรณ์ ผู้โจมตีสามารถส่งทราฟฟิกเครือข่ายที่ถูกสร้างขึ้นเป็นพิเศษไปยังระบบที่มีการใช้งานบริการDHCP หากโจมตีสำเร็จอาจนำไปสู่การรันโค้ดผ่านเครือข่ายโดยไม่ได้รับอนุญาต และส่งผลกระทบอย่างรุนแรงต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล

ช่องโหว่นี้มีความเสี่ยงสูง เนื่องจาก DHCP เป็นบริการพื้นฐานสำคัญของระบบเครือข่าย การโจมตีที่สำเร็จอาจนำไปสู่การยึดเซิร์ฟเวอร์ การติดตั้งมัลแวร์ การขโมยข้อมูล การหยุดชะงักของบริการ และการเคลื่อนที่ไปยังระบบอื่นภายในเครือข่าย ดังนั้นระบบที่เกี่ยวข้องกับทราฟฟิก DHCP ควรได้รับการติดตั้งแพตช์เป็นลำดับแรก

การข้ามกลไกความปลอดภัยของ Windows BitLocker

Microsoft ยังได้ออกแพตช์แก้ไข CVE-2026-45585 (คะแนน CVSS: 6.8) ซึ่งเป็นช่องโหว่ข้ามกลไกความปลอดภัยของ Windows BitLocker โดยก่อนหน้านี้นักวิจัยด้านความปลอดภัย Chaotic Eclipse (หรือ Nightmare-Eclipse) ได้เผยแพร่ PoC Exploit ภายใต้ชื่อ YellowKey เมื่อเดือนที่ผ่านมา

CVE-2026-45585 เป็นหนึ่งในหลายช่องโหว่ด้านการข้ามกลไกความปลอดภัยที่Microsoft แก้ไขในเดือนนี้ ได้แก่

- CVE-2026-45655 (คะแนน CVSS: 5.3)
- CVE-2026-45658 (คะแนน CVSS: 7.8)
- CVE-2026-50507 (คะแนน CVSS: 6.8)

Microsoft ระบุในคำแนะนำด้านความปลอดภัยว่า ผู้โจมตีที่ประสบความสำเร็จสามารถข้ามการป้องกันของBitLocker Device Encryption บนอุปกรณ์จัดเก็บข้อมูลของระบบได้ ผู้โจมตีที่สามารถเข้าถึงเครื่องเป้าหมายทางกายภาพ อาจใช้ช่องโหว่นี้เพื่อเข้าถึงข้อมูลที่ถูกเข้ารหัสไว้ ตามข้อมูลจากนักวิจัยด้านความปลอดภัย Will Dormann พบว่า CVE-2026-50507 ถูกประเมินว่าเป็นการแก้ไขช่องโหว่BitLocker Bypass ที่มีชื่อว่า bitskrieg ซึ่งสามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสได้ทั้งหมด

ช่องโหว่ Zero-Day และเทคนิคโจมตีแบบ HTTP2/Bomb

ทั้งนี้ CVE-2026-50507 รวมถึง CVE-2026-49160และ CVE-2026-45586 ถูกระบุว่าเป็น Zero-Dayที่มีการเปิดเผยต่อสาธารณะแล้ว

- CVE-2026-45586 (คะแนน CVSS: 7.8) - ช่องโหว่ยกระดับสิทธิ์ใน Windows Collaborative Translation Framework (CTFMON)
- CVE-2026-49160 (คะแนน CVSS: 7.5) - ช่องโหว่ Denial-of-Service ใน HTTP.sys

CVE-2026-49160 มีความเกี่ยวข้องกับเทคนิคการโจมตีที่เรียกว่าHTTP2/Bomb ซึ่งสามารถใช้ทำให้เว็บเซิร์ฟเวอร์หยุดให้บริการได้ภายในเวลาไม่กี่วินาที จากการทดสอบของ Calif พบว่า IIS Server ที่มีหน่วยความจำ 64 GB สามารถใช้ RAMจนหมดภายในเวลาประมาณ 45 วินาที เพื่อลดความเสี่ยงจากการโจมตีดังกล่าวMicrosoft ได้เพิ่ม Registry Setting ใหม่ชื่อ "MaxHeadersCount" เพื่อจำกัดจำนวน Header ที่อนุญาตในคำขอแบบ HTTP/2 และ HTTP/3

Microsoft อธิบายว่า การจำกัดจำนวน HTTP Header สามารถช่วยปกป้องระบบและเซิร์ฟเวอร์จากการใช้หน่วยความจำมากเกินไป การใช้ CPUสูงผิดปกติ และการโจมตีแบบปฏิเสธการให้บริการ เนื่องจาก HTTP/2 (HPACK) และ HTTP/3 (QPACK) ใช้เทคนิคการบีบอัดHeader และมีกระบวนการประมวลผลโปรโตคอลที่ซับซ้อนมากขึ้น การกำหนดขีดจำกัดของ Header เช่น MaxHeadersCount จึงช่วยรักษาประสิทธิภาพและความเสถียรของระบบได้

ในอีกด้านหนึ่ง CVE-2026-45586 ถูกคาดว่าเป็นการแก้ไขช่องโหว่Zero-Day สำหรับการยกระดับสิทธิ์ ซึ่ง Chaotic Eclipse ได้เปิดเผยภายใต้ชื่อ GreenPlasma ท้ายที่สุด การอัปเดตประจำเดือนมิถุนายน 2026 ยังได้แก้ไขMiniPlasma ซึ่งเป็นช่องโหว่อีกตัวหนึ่งที่ Chaotic Eclipse เปิดเผย โดยระบุว่าเป็นการแก้ไขที่ยังไม่สมบูรณ์ของ CVE-2020-17103ซึ่ง Microsoft เคยแก้ไขไปแล้วเมื่อเดือนธันวาคม2020

Microsoft ระบุเพิ่มเติมในคำแนะนำว่า เพื่อแก้ไขช่องโหว่ที่เกี่ยวข้องกับCVE-2020-17103 อย่างครบถ้วน ซึ่งล่าสุดถูกเรียกในที่สาธารณะว่า 'MiniPlasma' Microsoft แนะนำให้ติดตั้งอัปเดตประจำเดือนมิถุนายน 2026 สำหรับระบบปฏิบัติการ Windows

ผลกระทบของเทคโนโลยี AI ต่อการค้นพบช่องโหว่

จำนวนแพตช์ที่เพิ่มขึ้นอย่างต่อเนื่องในช่วงหลัง ถูกมองว่าเป็นผลจากการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในการค้นหาช่องโหว่ ซึ่ง Microsoft เชื่อว่าแนวโน้มนี้จะยังคงดำเนินต่อไปในอนาคตอันใกล้

Satnam Narang นักวิจัยอาวุโสจาก Tenable กล่าวว่า กล่องแพนโดราถูกเปิดออกแล้ว และเมื่อโมเดล AI ที่มีความสามารถสูงขึ้นเริ่มถูกใช้งานอย่างแพร่หลาย เราคาดว่าจำนวนช่องโหว่ที่ถูกค้นพบจะเพิ่มขึ้นอย่างต่อเนื่อง ไม่ใช่เฉพาะใน Patch Tuesday เท่านั้น

ขณะที่ Dustin Childs หัวหน้าฝ่ายThreat Awareness ของ TrendAI's Zero Day Initiative (ZDI) มองว่าจำนวนช่องโหว่จำนวนมหาศาลในครั้งนี้ เป็นตัวอย่างที่ชัดเจนว่า AI กำลังเร่งการค้นพบช่องโหว่ในระดับที่ยากจะควบคุม Childs กล่าวว่าจำนวน CVE ที่ Microsoftเผยแพร่ตั้งแต่ต้นปีนี้ สูงกว่าจำนวน CVE ทั้งหมดที่บริษัทเผยแพร่ตลอดทั้งปี2018 ไปแล้ว นับว่าเป็นเรื่องที่น่าทึ่งที่ Microsoftสามารถจัดทำแพตช์จำนวนมากขนาดนี้ได้ภายในเดือนเดียว และผมเชื่อว่าผู้ที่ทำหน้าที่ทดสอบแพตช์จำนวนไม่น้อย กำลังตั้งคำถามเกี่ยวกับคุณภาพของการทดสอบและผลกระทบที่อาจเกิดขึ้น

ขณะเดียวกัน Chaotic Eclipse ยังได้เผยแพร่PoC Exploit สำหรับ Zero-Day ตัวใหม่ของMicrosoft Defender ที่ใช้ชื่อว่า RoguePlanet โดยระบุว่าเป็นช่องโหว่ประเภท Race Condition ที่สามารถถูกใช้เพื่อเปิดWindows Command Prompt ด้วยสิทธิ์ระดับ SYSTEM ได้

ข้อมูลอ้างอิง

Jun 10, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/microsoft-patches-record-206-flaws.html