วันที่ 12 ธันวาคม 2568

Microsoft ออกแพตช์อุดช่องโหว่ 56 รายการ รวมถึงช่องโหว่ที่ถูกโจมตีจริงและอีกสองช่องโหว่แบบ Zero-Day

ไมโครซอฟท์ได้ออกอัปเดตความปลอดภัยประจำเดือนสุดท้ายของปี 2025 เพื่อแก้ไขช่องโหว่รวม 56 รายการ ในผลิตภัณฑ์ต่าง ๆ บนแพลตฟอร์ม Windows ซึ่งรวมถึงช่องโหว่ที่ถูกใช้งานโจมตีจริง (In-the-Wild Exploited Zero-Day) และช่องโหว่ Zero-Day ที่ถูกเปิดเผยต่อสาธารณะแล้ว

- สรุปสถิติ Patch: มีช่องโหว่ระดับวิกฤต (Critical) 3 รายการ และระดับสำคัญ (Important) 53 รายการ นอกจากนี้มีช่องโหว่ที่ถูกเปิดเผยสู่สาธารณะแล้ว (Publicly Disclosed) อีก 2 รายการ
- การจำแนกประเภท: การยกระดับสิทธิ์ 29 รายการ, การรันโค้ดจากระยะไกล 18 รายการ, การเปิดเผยข้อมูล 4 รายการ, DoS 3 รายการ และการปลอมแปลงข้อมูล 2 รายการ
- สถิติรวมปี 2025: ไมโครซอฟท์ได้แก้ไขช่องโหว่ไปทั้งหมด 1,275 รายการ ในปีนี้ ซึ่งเป็นปีที่สองติดต่อกันที่จำนวนช่องโหว่เกิน 1,000 รายการ

ช่องโหว่ Zero-Day ที่ถูกใช้โจมตีจริง (In-the-Wild Exploited)

ช่องโหว่ที่ร้ายแรงที่สุดในชุดแพตช์นี้คือ:

- CVE-2025-62221 (CVSS: 7.8): ช่องโหว่แบบ Use-after-free ใน Windows Cloud Files Mini Filter Driver ช่องโหว่นี้ช่วยให้ผู้โจมตีที่มีสิทธิ์อยู่แล้วสามารถ ยกระดับสิทธิ์ขึ้นเป็น SYSTEM ได้

บริบททางเทคนิค:

- Cloud Files Mini Filter Driver: คอมโพเนนต์นี้ถูกใช้โดย OneDrive, Google Drive, iCloud และเป็นคอมโพเนนต์มาตรฐานของ Windows ที่ติดตั้งอยู่แล้ว

- CISA KEV List: การถูกใช้งานจริงทำให้ CISA เพิ่มช่องโหว่นี้ลงในบัญชี Known Exploited Vulnerabilities (KEV) และบังคับให้หน่วยงาน FCEB ต้องอัปเดตก่อนวันที่ 30 ธันวาคม 2025

สองช่องโหว่ Zero-Day ที่ถูกเปิดเผยสู่สาธารณะ (Publicly Disclosed)

อัปเดตนี้ยังแก้ไขช่องโหว่ที่ถูกเปิดเผยต่อสาธารณะแล้วอีก 2 รายการ:

1. CVE-2025-54100 (CVSS: 7.8) – Command Injection ใน Windows PowerShell

- ลักษณะ: ช่องโหว่ Command Injection ในกระบวนการที่ PowerShell จัดการเนื้อหาเว็บ
- กลไกการโจมตี: ผู้โจมตีที่ไม่ได้รับสิทธิ์สามารถรันโค้ดภายในเครื่อง ตามสิทธิ์ของผู้ใช้ปัจจุบันที่เรียกใช้คำสั่งที่ถูกสร้างขึ้น เช่น Invoke-WebRequest โดยการหลอกให้ผู้ใช้รันคำสั่งที่ชี้ไปยังเซิร์ฟเวอร์ผู้โจมตี

2. CVE-2025-64671 (CVSS: 8.4) – Command Injection ใน GitHub Copilot for JetBrains

- ลักษณะ: ช่องโหว่ Command Injection เป็นส่วนหนึ่งของกลุ่มช่องโหว่ IDEsaster
- กลไกการโจมตี: เกิดจากการโจมตีแบบ Cross Prompt Injection ซึ่งเป็นการดัดแปลงพรอมต์ที่ตัว LLM สร้างขึ้นเอง โดยอาศัยค่าตั้งค่า 'อนุมัติโดยอัตโนมัติ' ของผู้ใช้ ทำให้รันโค้ดได้ (กระทบ IDE อื่น ๆ เช่น Cursor, JetBrains Junie, Gemini CLI, และ Roo Code)

อัปเดตอื่น ๆ ที่เกี่ยวข้อง

- Microsoft Edge (Chromium): มีการแก้ไขปัญหา 17 รายการ รวมถึงช่องโหว่แบบปลอมแปลงบน Edge for iOS (CVE-2025-62223, CVSS: 4.3)
- แพตช์จากผู้ให้บริการรายอื่น: ผู้ให้บริการรายอื่น ๆ อีกมากมายออกอัปเดตเพื่อแก้ไขช่องโหว่ในช่วงหลายสัปดาห์ที่ผ่านมา ได้แก่: Adobe, Amazon Web Services, AMD, Arm, Atlassian, Broadcom (VMware), Cisco, Dell, F5, Fortinet, GitLab, Google (Android, Chrome, Cloud), HP, IBM, Intel, Ivanti, Linux distributions, MongoDB, Mozilla Firefox, NVIDIA, Qualcomm, React, Samsung, SAP, Schneider Electric, Siemens, SolarWinds, Splunk, Synology, Zyxel และอีกหลายราย

ข้อมูลอ้างอิง

Dec 10, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/12/microsoft-issues-security-fixes-for-56.html