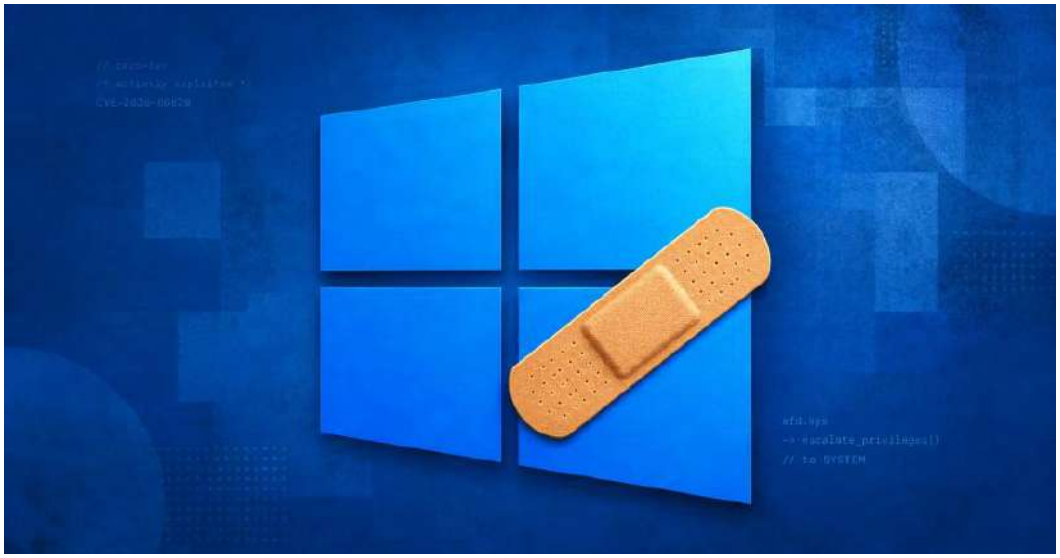
วันที่ 17 สิงหาคม 2569

Microsoft ออกแพตช์แก้ไขช่องโหว่ 398 รายการ รวมถึง Zero-Day ในไดรเวอร์ Windows ที่กำลังถูกใช้โจมตี



Microsoft ได้ออกอัปเดตความปลอดภัยประจำเดือนเมื่อวันอังคารที่ผ่านมา โดยหนึ่งในช่องโหว่ที่ได้รับการแก้ไขกำลังถูกนำไปใช้ในการโจมตีแล้ว ช่องโหว่นี้อยู่ในไดรเวอร์หลักของ Windows ที่ทำหน้าที่จัดการการทำงานของ network socket โดยผู้โจมตีที่สามารถรันโค้ดบนเครื่องเป้าหมายได้อยู่แล้ว สามารถใช้ช่องโหว่นี้เพื่อยกระดับสิทธิ์เป็น SYSTEM ได้ ดังนั้นช่องโหว่นี้จึงควรถูกจัดการเป็นอันดับแรก

ช่องโหว่นี้มีหมายเลข CVE-2026-68820 (CVSS score: 7.0) และเป็นช่องโหว่เพียงรายการเดียวในการอัปเดตประจำเดือนนี้ที่ Microsoft ระบุว่ากำลังถูกนำไปใช้โจมตีอยู่ การโจมตีต้องอาศัยการทำให้เกิด race condition ในไดรเวอร์ โดย Microsoft ยังไม่ได้ระบุว่ากลุ่มใดเป็นผู้โจมตี ขณะที่ Check Point Research ระบุว่า Lazarus ใช้ Zero-Day นี้ในการโจมตีในแคมเปญ Operation Dream Job

ช่องโหว่อีก 4 รายการในการอัปเดตครั้งนี้ไม่ต้องอาศัยการดำเนินการใดๆ จากเหยื่อเลย ไม่ต้องมีบัญชีผู้ใช้ ไม่ต้องใช้รหัสผ่าน และไม่ต้องให้เหยื่อคลิกอะไร ช่องโหว่เหล่านี้ส่งผลกระทบต่อ Windows DNS Server, Windows Deployment Services, การใช้งานโปรโตคอล QUIC ของ Microsoft และ High Performance Computing (HPC) Pack โดยแต่ละช่องโหว่มีคะแนน CVSS 9.8 และไม่มีรายการใดถูกระบุว่ากำลังถูกนำไปใช้โจมตีในขณะที่มีการเผยแพร่อัปเดต

เมื่อแยกนับตามรายการ Zero Day Initiative ระบุว่าการอัปเดตครั้งนี้ครอบคลุม CVE ใหม่ทั้งหมด 398 รายการ โดย 62 รายการถูกจัดอยู่ในระดับ Critical จำนวนดังกล่าวสะท้อนให้เห็นถึงขนาดของการอัปเดต แต่สถานะการถูกโจมตีและขอบเขตของระบบที่ได้รับผลกระทบเป็นปัจจัยสำคัญในการกำหนดลำดับความเร่งด่วนของการติดตั้งแพตช์

การอัปเดตครั้งนี้ยังแก้ไขส่วน RCE ของช่องโหว่ที่ใช้โจมตี SharePoint เป็นชุด ซึ่งช่องโหว่สำหรับหลบเลี่ยงการตรวจสอบสิทธิ์ได้รับการแก้ไขไปแล้วในเดือนกรกฎาคม ดังนั้นระบบ SharePoint แบบติดตั้งภายในองค์กรควรติดตั้งอัปเดตทั้งสองรายการให้เรียบร้อย

Check Point Research ระบุว่า CVE-2026-68820 เป็นช่องโหว่ use-after-free ใน afd.sys หรือ Ancillary Function Driver for WinSock ซึ่งเป็นส่วนประกอบของ Windows ที่ทำงานอยู่ในระดับ Kernel และเกี่ยวข้องกับการทำงานด้านเครือข่ายของ Windows

ช่องโหว่นี้เป็นช่องโหว่สำหรับยกระดับสิทธิ์ โดยผู้โจมตีจำเป็นต้องสามารถรันโค้ดบนเครื่องได้ก่อน จากนั้นจึงใช้ช่องโหว่นี้เพื่อยกระดับสิทธิ์ไปเป็น SYSTEM Microsoft ระบุว่าช่องโหว่นี้กำลังถูกนำไปใช้โจมตีอยู่จริง ทำให้ต้องให้ความสำคัญก่อนช่องโหว่ RCE ทั้ง 4 รายการที่มีคะแนน 9.8 แม้ว่าคะแนนของช่องโหว่นี้จะต่ำกว่าก็ตาม

ช่องโหว่ Remote Code Execution (RCE) ทั้ง 4 รายการที่ไม่ต้องมีการยืนยันตัวตน เป็นช่องโหว่ที่ควรจัดลำดับความสำคัญรองจากช่องโหว่ในไดรเวอร์ที่กำลังถูกใช้โจมตี เนื่องจากผู้โจมตีสามารถใช้ช่องโหว่เหล่านี้เพื่อรันโค้ดบนเซิร์ฟเวอร์ได้ โดยไม่จำเป็นต้องมีบัญชีผู้ใช้หรือให้เหยื่อดำเนินการใดๆ

- CVE-2026-62878 Windows DNS Server เป็นช่องโหว่ stack-based buffer overflow ที่สามารถโจมตีจากระยะไกลได้โดยไม่ต้องผ่านการยืนยันตัวตนและไม่ต้องมีการโต้ตอบจากผู้ใช้ Zero Day Initiative ระบุว่าช่องโหว่นี้มีเงื่อนไขทางเทคนิคที่สามารถแพร่กระจายแบบ worm ได้ แม้ Microsoft จะประเมินว่าโอกาสที่จะถูกนำไปใช้โจมตีนั้นอยู่ในระดับต่ำกว่า ทั้งนี้ คำว่า “wormable” ของ ZDI เป็นการอธิบายลักษณะทางเทคนิคของช่องโหว่ไม่ได้หมายความว่ามีการพบมัลแวร์ที่แพร่กระจายแบบ Worm แล้ว
- CVE-2026-62893 Windows Deployment Services เป็นช่องโหว่ที่สามารถโจมตีจากระยะไกลผ่านการทำงานของบริการ TFTP โดยไม่ต้องมีการยืนยันตัวตนหรือการโต้ตอบจากผู้ใช้
- CVE-2026-62815 Microsoft QUIC เป็นช่องโหว่ Remote Code Execution ที่สามารถโจมตีจากระยะไกลได้โดยไม่ต้องผ่านการยืนยันตัวตนและไม่ต้องมีการโต้ตอบจากผู้ใช้
- CVE-2026-59124 HPC Pack มีคะแนน CVSS 9.8 เช่นเดียวกัน แต่ถูกจัดอยู่ในระดับ Important แทนที่จะเป็น Critical เนื่องจาก HPC Pack ไม่ได้ติดตั้งมาเป็นค่าเริ่มต้น และ Microsoft ประเมินว่าโอกาสที่ช่องโหว่นี้จะถูกนำไปใช้โจมตีนั้นอยู่ในระดับสูงกว่า

HPC Pack ไม่ได้ติดตั้งมาเป็นค่าเริ่มต้น และความสำคัญของอีก 3 ช่องโหว่ก็ขึ้นอยู่กับว่าบริการที่มีช่องโหว่นั้นถูกติดตั้งและสามารถเข้าถึงจากภายนอกได้หรือไม่ ดังนั้นการตรวจสอบว่ามีบริการดังกล่าวอยู่ในระบบหรือไม่ รวมถึงการตรวจสอบว่าสามารถเข้าถึงได้จากเครือข่ายใด จึงมีความสำคัญพอๆ กับสถานะการถูกนำไปใช้โจมตีเมื่อกำหนดลำดับความสำคัญในการติดตั้งแพตช์

การอัปเดตในเดือนสิงหาคมยังเป็นการปิดช่องโหว่ SharePoint ที่เกี่ยวข้องกัน 2 ส่วน ซึ่งเริ่มต้นจากการแก้ไขในเดือนกรกฎาคม

Rapid7 Labs รายงานช่องโหว่ที่สามารถนำมาใช้ร่วมกันเป็นชุดให้ Microsoft ทราบเมื่อวันที่ 18 พฤษภาคม โดยเป็นการใช้ช่องโหว่สำหรับหลบเลี่ยงการตรวจสอบสิทธิ์ร่วมกับช่องโหว่สำหรับรันโค้ดอีกหนึ่งรายการ เพื่อโจมตี SharePoint ที่ติดตั้งภายในองค์กรจนสามารถรันโค้ดจากระยะไกลได้โดยไม่ต้องผ่านการยืนยันตัวตน Microsoft ยืนยันในอีกสองวันต่อมาว่าจะแบ่งการแก้ไขออกเป็นการอัปเดตในเดือนกรกฎาคมและสิงหาคม

การอัปเดตในเดือนกรกฎาคมได้แก้ไขช่องโหว่ส่วนแรกแล้ว คือ CVE-2026-55040 ซึ่งเป็นช่องโหว่ Critical สำหรับหลบเลี่ยงการตรวจสอบสิทธิ์ โดยมีคะแนน 9.1 Rapid7 พบว่าช่องโหว่นี้ทำให้ผู้โจมตีจากระยะไกลที่ไม่ต้องผ่านการยืนยันตัวตนสามารถปลอมเป็นผู้ใช้หรือผู้ดูแลระบบของ SharePoint ได้ หากผู้โจมตีทราบตัวตนของบัญชีที่ต้องการปลอมเป็น ส่วนการอัปเดตในเดือนสิงหาคมได้แก้ไขส่วนของ RCE ซึ่งระบุเป็น CVE-2026-63520

ความแตกต่างนี้มีความสำคัญ เนื่องจาก CVE-2026-63520 เป็นช่องโหว่ในส่วนของการรันโค้ด ไม่ใช่ช่องโหว่ที่ทำให้สามารถเข้าถึงระบบโดยไม่ต้องยืนยันตัวตนได้ด้วยตัวมันเอง การนำ CVE-2026-63520 มาใช้ร่วมกับ CVE-2026-55040 จึงเป็นสิ่งที่ทำให้ Rapid7 สามารถโจมตี SharePoint และรันโค้ดจากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตนได้

Rapid7 ระบุว่าการติดตั้งแพตช์สำหรับ CVE-2026-55040 สามารถตัดเส้นทางการโจมตีที่แสดงให้เห็นออกไปได้ ดังนั้นเมื่อมีการติดตั้งแพตช์ของเดือนกรกฎาคมแล้ว เส้นทางการโจมตีดังกล่าวก็ถูกปิดไปก่อนหน้านี้แล้ว ส่วนการอัปเดตในเดือนสิงหาคมจะช่วยปิดช่องโหว่ในส่วนของ RCE ให้สมบูรณ์ยิ่งขึ้น

สำหรับการจัดลำดับความสำคัญ ควรให้ CVE-2026-68820 เป็นอันดับแรกในระบบ Windows ที่ผู้โจมตีอาจสามารถรันโค้ดบนเครื่องได้อยู่แล้วและสามารถใช้ช่องโหว่นี้เพื่อยกระดับสิทธิ์เป็น SYSTEM จากนั้นให้เร่งตรวจสอบและติดตั้งแพตช์สำหรับบริการ DNS, WDS, QUIC และ HPC ที่เปิดให้เข้าถึงจากภายนอก และตรวจสอบให้แน่ใจว่า SharePoint แบบติดตั้งภายในองค์กรได้รับการติดตั้งทั้งแพตช์แก้ไขช่องโหว่สำหรับหลบเลี่ยงการตรวจสอบสิทธิ์ในเดือนกรกฎาคม และแพตช์แก้ไขช่องโหว่ RCE ในเดือนสิงหาคมเรียบร้อยแล้ว

ข้อมูลอ้างอิง

Aug 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/microsoft-patches-398-flaws-including.html