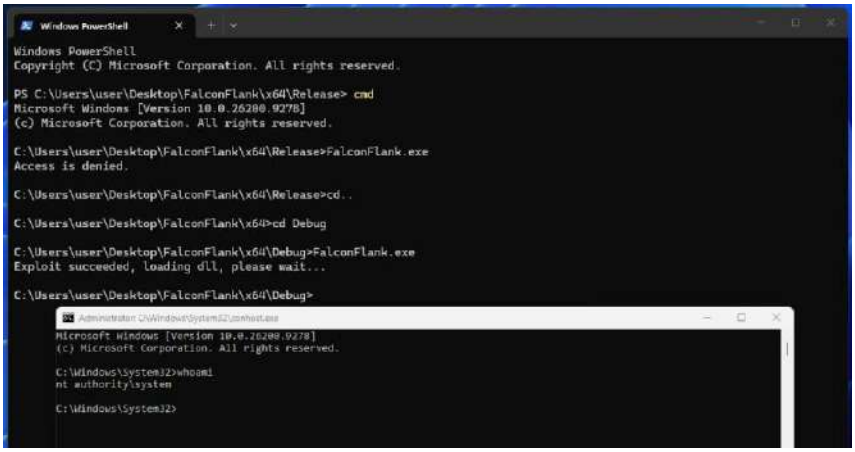
วันที่ 4 กันยายน 2569

Researcher Releases FalconFlank PoC Showing Privilege Escalation in CrowdStrike Falcon



นักวิจัยด้านความปลอดภัยที่รู้จักกันในชื่อ Chaotic Eclipse (หรือ INFINITE NIGHTMARE, MSNightmare และ Nightmare-Eclipse) ได้เผยแพร่ zero-day ตัวใหม่ที่มีชื่อว่า FalconFlank ซึ่งเป็น Proof-of-Concept (PoC) สำหรับช่องโหว่การยกระดับสิทธิ์ (Privilege Escalation) ที่ส่งผลกระทบต่อ CrowdStrike Falcon

FalconFlank เป็น 0-day ที่ทำให้สามารถยกระดับสิทธิ์ได้ โดยอาศัยการทำงานของฟีเจอร์สำหรับจัดการ Office macro ที่เป็นอันตรายของ CrowdStrike Falcon Sensor นักวิจัยระบุไว้ในไฟล์ README บน GitHub พร้อมระบุว่า บริษัทด้านความปลอดภัยทางไซเบอร์อาจมีระบบตรวจจับช่องโหว่นี้อยู่แล้วในขณะนี้ ดังนั้นหากต้องการทดสอบ คุณอาจจำเป็นต้องเพิ่ม PoC เข้าไปใน exclusions หรือทำการ obfuscate PoC และเปลี่ยนเทคนิคที่ใช้ในการโหลด DLL

นักวิจัยระบุเพิ่มเติมว่า PoC ดังกล่าวสามารถทำงานได้บนเครื่อง Windows 11 25H2 ที่ได้รับการอัปเดตล่าสุด หรือ Windows Server 2025 ที่ติดตั้ง CrowdStrike Falcon ในแถลงการณ์ที่ส่งให้กับ The Hacker News

โฆษกของ CrowdStrike ระบุว่า บริษัทกำลังตรวจสอบรายงานดังกล่าวอยู่ในขณะนี้ เรากำลังตรวจสอบข้อกล่าวอ้างดังกล่าวอย่างต่อเนื่อง และแนะนำให้ลูกค้าปิดการตั้งค่า Windows policy Microsoft Office File Suspicious Macro Removal ลูกค้ายังคงได้รับการป้องกันผ่านการตั้งค่า Cloud Anti-malware for Microsoft Office Files โดยสามารถดูรายละเอียดเพิ่มเติมได้จาก FalconFlank Tech Alert ใน CrowdStrike Support Portal

ตาม Tech Alert ของ CrowdStrike ที่เผยแพร่เมื่อวันที่ 3 กันยายน 2026 บริษัทระบุว่ากำลังตรวจสอบข้อกล่าวอ้างเกี่ยวกับ FalconFlank และทีม Counter Adversary Operations และ OverWatch กำลังค้นหาสัญญาณที่อาจบ่งชี้ถึงการถูกใช้ประโยชน์จากช่องโหว่นี้อยู่ด้วย

การเปิดเผยดังกล่าวเกิดขึ้นเพียงไม่กี่วันหลังจาก Chaotic Eclipse เผยแพร่ PoC สำหรับช่องโหว่การยกระดับสิทธิ์อีกหนึ่งรายการ ซึ่งส่งผลกระทบต่อผลิตภัณฑ์รักษาความปลอดภัยปลายทางของ Kaspersky สำหรับ Windows เวอร์ชัน 14.0.0.504 โดยช่องโหว่นี้มีชื่อว่า HardBreacher

PoC นี้ยังอยู่ในสภาพที่ไม่สมบูรณ์มากนัก โดยพื้นฐานแล้วเป็นการนำหลายส่วนมาประกอบกันเพื่อให้มันทำงานได้ และผมเพียงแค่ทำให้มันสามารถใช้งานได้เท่านั้น นักวิจัยกล่าว

PoC อาจทำงานล้มเหลวและแสดง error ดังนั้นคุณอาจต้องลองรันซ้ำ หากทำงานสำเร็จ มันจะสร้างไฟล์ที่ C:\Windows\System32\MY_SNAKE_IS_SOLID.dll พร้อมกำหนดสิทธิ์แบบเต็มให้กับผู้ใช้ปัจจุบัน

ส่วนที่น่าสนใจคือ Kaspersky จะมีปัญหาอย่างมากเมื่อคุณสามารถควบคุม UI process ได้ คุณสามารถทำให้ระบบหยุดทำงาน ให้หรือปฏิเสธการเข้าถึงไฟล์ที่ไม่ควรเข้าถึงได้ และหาก PoC ทำงานสำเร็จ ระบบปฏิบัติการทั้งหมดก็อาจเกิดความผิดปกติอย่างรุนแรง

เมื่อ The Hacker News ติดต่อไปยัง Kaspersky บริษัทระบุว่าได้แก้ไขปัญหา HardBreacher แล้ว การแก้ไขที่เกี่ยวข้องถูกส่งผ่าน automatic update แล้ว หรือผู้ใช้สามารถสั่งอัปเดตฐานข้อมูลด้วยตนเองได้ บริษัทระบุ

เมื่อเดือนที่ผ่านมา นักวิจัยรายเดียวกันยังได้เผยแพร่ PoC สำหรับ zero-day ของ Microsoft Defender ที่มีชื่อว่า ShieldBreak หรือ CVE-2026-69414 ซึ่งอาจเปิดโอกาสให้ผู้โจมตีสามารถเรียกใช้โค้ดที่กำหนดเองด้วยสิทธิ์ NT AUTHORITY\SYSTEM

ช่องโหว่นี้ถูกประเมินว่าเป็นการ bypass การแก้ไขสำหรับ CVE-2026-50656 หรือที่รู้จักกันในชื่อ RoguePlanet โดย Microsoft ยังไม่ได้เผยแพร่แพตช์สำหรับปัญหาดังกล่าว เช่นเดียวกับช่องโหว่ก่อนหน้านี้ ShieldBreak สำรวจอีกส่วนหนึ่งของระบบปฏิบัติการ Windows

ในขณะที่ RedSun ใช้ประโยชน์จาก Cloud Files API และ TieringEngineService เพื่อเปลี่ยนเส้นทางการเขียนของ Defender ไปยัง System32 และ LegacyHive ใช้การจัดการ registry hive แบบ offline ร่วมกับ Windows NT Object Manager namespace แต่ ShieldBreak ผสานการทำงานของ Cloud Files, Object Manager namespace, การเรียกใช้ Windows Defender API โดยตรง และ timing race ใน remediation path

ผลลัพธ์คือการโจมตีแบบ local privilege escalation ที่สามารถทำงานได้ด้วยตัวเอง โดยเปลี่ยนเส้นทางการทำงานของ Windows Defender ไปเขียน DLL ที่ผู้โจมตีควบคุมไปยัง C:\Windows\System32\phoneinfo.dll จากนั้นจึงทำให้เกิดการทำงานด้วยสิทธิ์ SYSTEM ผ่าน Windows Error Reporting task ที่มีอยู่ในระบบ

หลังจากนั้นไม่นาน นักวิจัยอ้างว่า Microsoft ยังคงไม่ตอบกลับและปฏิเสธที่จะติดต่อสื่อสารในรูปแบบใดๆ โดยระบุว่า Microsoft “พยายามอย่างมากที่จะทำให้ผมดูเหมือนเป็นอาชญากรที่เสียสติ”

“ผมไม่สามารถรายงานบั๊กที่พบให้กับผู้ผลิตที่เกี่ยวข้องได้ด้วยซ้ำ เนื่องจากข้อจำกัดจาก Microsoft ทั้งหมดนี้เป็นสิ่งที่พวกเขาสร้างขึ้นเอง และคุณรู้ไหมว่า พวกเขายังไม่แม้แต่จะตรวจสอบเคสของผมเพื่อดูว่าเกิดอะไรขึ้น”

“ผมคิดว่าผมจะเริ่มเผยแพร่บั๊กของผลิตภัณฑ์จากผู้ผลิตรายอื่นในช่วงเวลาที่ Patch Tuesday ยังไม่ออก ผมแค่อยากใช้ชีวิตเหมือนคนปกติสักครั้ง มันมากเกินไปที่จะขอหรือ...?”

Update

Chaotic Eclipse ยังได้เผยแพร่ PoC สำหรับช่องโหว่ memory corruption ใน NVIDIA ที่มีชื่อว่า GreenSection และช่องโหว่ privilege escalation ในซอฟต์แวร์ป้องกันไวรัส Avast ของ Gen Digital ที่มีชื่อว่า PrettyPrague

GreenSection ทำให้แอปพลิเคชันใดๆ ที่ใช้ Vulkan หรือ OpenGL เกิด crash หลังจากรัน PoC

“PoC จะ dump ฐานข้อมูล SAM โดยอาศัยช่องโหว่ใน Avast Sandbox และสร้าง full SYSTEM shell โดยในขณะที่เขียนรายงานนี้ PoC ยังสามารถทำงานได้บน Avast Antivirus ที่ได้รับการแพตช์แล้ว และ Windows 11 25H2 ที่ได้รับการแพตช์แล้ว” “ผมไม่แน่ใจ แต่ผมเชื่อว่าช่องโหว่นี้อาจส่งผลกระทบต่อผลิตภัณฑ์อื่นๆ ของ Gen Digital ด้วย เช่น AVG และ Norton”

(เรื่องนี้ได้รับการอัปเดตหลังจากเผยแพร่ครั้งแรก เพื่อเพิ่มคำชี้แจงจาก CrowdStrike และ Kaspersky)

ข้อมูลอ้างอิง

Sep 3, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/09/researcher-releases-falconflank-poc.html