วันที่ 15 มิถุนายน 2569

GreatXML ช่องโหว่ใหม่ที่สามารถข้ามการป้องกันของ Windows BitLocker ผ่านไฟล์ XML ในพาร์ทิชัน Recovery

นักวิจัยด้านความปลอดภัยที่ใช้ชื่อว่า Chaotic Eclipse (หรือที่รู้จักในชื่อ Nightmare-Eclipse และ MSNightmare)ได้เปิดเผยเทคนิคใหม่สำหรับข้ามการป้องกันของ Windows BitLocker ซึ่งมีชื่อว่า GreatXML เพียงหนึ่งวันหลังจากที่เขาเผยแพร่ช่องโหว่สำหรับMicrosoft Defender นี่เป็นการค้นพบโดยบังเอิญ ใช้เวลาทั้งหมดเพียง 4 ชั่วโมงในการหาช่องโหว่นี้

นักวิจัยกล่าวในโพสต์บน Blogger ว่า “หากคุณเคยใช้ฟีเจอร์ Windows Defender Offline Scan มาก่อน เครื่องของคุณจะมีความเสี่ยงต่อการถูกข้ามการป้องกันของ BitLocker โดยอัตโนมัติ ผมยังไม่แน่ใจว่าช่องโหว่นี้จะยังสามารถถูกกระตุ้นได้หรือไม่ หากไม่เคยใช้ฟีเจอร์ Offline Scan มาก่อน แต่มีความเป็นไปได้ค่อนข้างมาก”

ขั้นตอนการทำงานของช่องโหว่

การทำงานของช่องโหว่มีขั้นตอนดังนี้:

- คัดลอกไฟล์ XML ชื่อ "unattend.xml" และโฟลเดอร์ Recovery ที่มีไฟล์ XML อีกไฟล์หนึ่งคือ Recovery/WindowsRE/ReAgent.xml ไปไว้ที่ตำแหน่ง Root ของพาร์ทิชัน Recovery
- รีสตาร์ตเครื่องเข้าสู่ Windows Recovery Environment (WinRE) โดยกดปุ่ม Shift ค้างไว้ แล้วคลิก Restart จากเมนูพลังงานของ Windows
- หากดำเนินการครบทุกขั้นตอนอย่างถูกต้อง ระบบจะเปิด Shell ขึ้นมาพร้อมสิทธิ์การเข้าถึงข้อมูลในไดรฟ์ที่ถูกป้องกันด้วย BitLocker ได้อย่างไม่มีข้อจำกัด

หากไม่เคยเรียกใช้งาน Defender Offline Scan มาก่อน คุณจะต้องล็อกอินเข้าเครื่องแล้วเปิดใช้งานด้วยตัวเอง หรือหาวิธีทำให้เครื่องบูตเข้า WinRE ในสถานะของ Offline Scan ซึ่งผมเชื่อว่าน่าจะสามารถทำได้โดยไม่จำเป็นต้องล็อกอินเข้าสู่ระบบและจากนั้นจึงทำตามขั้นตอนข้างต้น" Chaotic Eclipse กล่าว

ข้อโต้แย้งและจุดบกพร่องจากการทดสอบ

อย่างไรก็ตาม ในโพสต์บน Mastodon นักวิจัยด้านความปลอดภัย Will Dormann แสดงความเห็นว่าขั้นตอนการทดสอบและยืนยันช่องโหว่ GreatXMLยังมีข้อบกพร่องอยู่ โดยเขาระบุว่าการเปิดใช้งาน Microsoft Defender Offline Scan จำเป็นต้องให้ผู้ใช้ล็อกอินเข้าสู่ Windows และต้องมีสิทธิ์ผู้ดูแลระบบ (Administrator) ก่อน ซึ่งในสถานการณ์ดังกล่าว ผู้ใช้ก็สามารถปิดการทำงานของ BitLocker ได้อยู่แล้ว

บทความเกี่ยวกับ GreatXML ระบุว่าข้อกำหนดเบื้องต้นคือ ต้องเคยใช้งาน Windows Defender Offline มาก่อน และหลังจากนำไฟล์ทั้งสองไปวางใน WinRE แล้ว เพียงแค่กด Shiftพร้อมรีสตาร์ตเข้าสู่ WinRE ระบบก็จะเข้าสู่โหมดMicrosoft Defender Offline Scan โดยอัตโนมัติ แต่จากการทดสอบบน Windows 11 ทั้ง 3 สายการพัฒนาที่ผมมีอยู่ ไม่พบว่าพฤติกรรมดังกล่าวเกิดขึ้น

ความเชื่อมโยงกับช่องโหว่อื่นๆ ที่ถูกค้นพบ

การเปิดเผย GreatXML เกิดขึ้นไม่นานหลังจากมีการเปิดเผย RoguePlanet ซึ่งเป็นช่องโหว่แบบ Zero-Day ใน Microsoft Defender ที่สามารถยกระดับสิทธิ์จากผู้ใช้ทั่วไปไปเป็น SYSTEM ได้ ส่งผลให้ผู้โจมตีสามารถรันโค้ดตามต้องการ หรือดำเนินการต่าง ๆ บนเครื่องได้โดยไม่ได้รับอนุญาต

GreatXML ยังถือเป็นช่องทางข้ามการป้องกันของ BitLockerตัวที่สองที่ถูกเปิดเผยโดย Chaotic Eclipse ต่อจาก YellowKey (หรือ CVE-2026-45585) ซึ่ง Microsoftได้ออกแพตช์แก้ไขแล้วในชุดอัปเดต Patch Tuesday ของสัปดาห์นี้.

ข้อมูลอ้างอิง

Jun 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/new-greatxml-exploit-bypasses-windows.html