ประจำวันพุธที่ 22 มิถุนายน 2565

# การโจมตี DFSCoerce NTLM Relay แบบใหม่ ที่ทำให้สามารถเข้าถึง Domain Windows ได้

การโจมตีแบบ DFSCoerce Windows NTLM ที่ใช้ MS-DFSNM ซึ่งเป็นระบบไฟล์แบบกระจายของ Microsoft เพื่อเข้าถึง Domain Windows โดยสมบูรณ์ ซึ่งหลายองค์กรใช้ Microsoft Active Directory Certificate Services ซึ่งเป็นบริการโครงสร้างพื้นฐานคีย์สาธารณะ (PKI) ที่ใช้ในการตรวจสอบสิทธิ์ผู้ใช้ บริการ และอุปกรณ์บน Domain Windows

บริการนี้เสี่ยงต่อการถูกโจมตีแบบรีเลย์ NTLM จะเกิดขึ้นเมื่อผู้โจมตีบังคับตัวควบคุม Domain เพื่อรับรองความถูกต้องกับการส่งต่อ NTLM ที่เป็นอันตรายภายใต้การควบคุมของผู้โจมตี เซิร์ฟเวอร์ที่เป็นอันตรายนี้จะส่งต่อหรือส่งต่อคำขอตรวจสอบสิทธิ์ไปยัง Active Directory Certificate Services ของ Domain ผ่าน HTTP และสุดท้ายจะได้รับ Kerberos Ticket-granting (TGT) ซึ่งจะอนุญาตให้ผู้โจมตีสามารถระบุตัวตนของอุปกรณ์ใด ๆ บนเครือข่าย รวมถึงตัวควบคุม Domain เมื่อควบคุม Domain แล้วจะมีสิทธิ์ยกระดับเพื่อให้ผู้โจมตีเข้าควบคุมโดเมนและเรียกใช้คำสั่งใดๆ ก็ได้

นักวิจัยแจ้งกับ BleepingComputer ถึงวิธีที่ดีที่สุดในการป้องกันการโจมตีประเภทนี้คือการปฏิบัติตามคำแนะนำของ Microsoft ในการป้องกันการโจมตีแบบรีเลย์ PetitPotam NTLM ให้ปิดใช้งาน NTLM บนตัวควบคุม Domain และการเปิดใช้งาน Extended Protection การรับรองความถูกต้องและคุณลักษณะการเซ็นชื่อ เช่น การลงนาม SMB เพื่อปกป้องข้อมูลประจำตัวของ Windows วิธีการป้องกันอื่นๆ รวมถึงการใช้ ตัวกรอง RPC ในตัวของ Windows หรือ ไฟร์วอลล์ RPC เพื่อป้องกันไม่ให้เซิร์ฟเวอร์ถูกบังคับผ่านโปรโตคอล MS-DFSNM

ที่มาของข่าว : https://www.bleepingcomputer.com/news/microsoft/new-dfscoerce-ntlm-relay-attack-allows-windows-domain-takeover/