ประจำวันจันทร์ที่ 27 มิถุนายน 2565

Mitel Zero-day ถูกนำไปใช้โดยแฮกเกอร์สำหรับการโจมตีด้วยแรนซัมแวร์

แฮกเกอร์ใช้ช่องโหว่แบบ Zero-day บนอุปกรณ์ Mitel MiVoice VOIP ที่ใช้ Linux สำหรับการเข้าถึงครั้งแรก ซึ่งเป็นจุดเริ่มต้นของการโจมตีแรนซัมแวร์ บนอุปกรณ์ Mitel VOIP ถูกใช้โดยองค์กรที่สำคัญในภาคส่วนต่างๆ สำหรับบริการโทรศัพท์ และได้เพิ่งถูกโจมตีไป

บริษัท CrowdStrike กล่าวว่าถึงช่องโหว่ในการเรียกใช้โค้ดจากระยะไกลแบบ zero-day ที่หมายเลข CVE-2022-29499 (คะแนน CVSS v3 : 9.8) ถูกนำมาใช้เพื่อเข้าถึงเครือข่ายในเบื้องต้น แม้ว่าการโจมตีจะหยุดลงแต่ CrowdStrike เชื่อว่า Zero-day จะถูกใช้เป็นส่วนหนึ่งของการโจมตีแรนซัมแวร์ ซึ่งช่องโหว่ Mitel Service Appliance ของ MiVoice Connect ซึ่งใช้ใน SA 100, SA 400 และ Virtual SA ทำให้ผู้โจมตีสามารถเรียกใช้โค้ดจากระยะไกล (RCE) และปัญหาเกิดจากการตรวจสอบข้อมูลไม่เพียงพอสำหรับสคริปต์ ทำให้ผู้โจมตีจากระยะไกลที่ไม่ผ่านการตรวจสอบสิทธิ์สามารถสั่งงานโดยใช้คำขอที่ออกแบบมาเป็นพิเศษ

ช่องโหว่เกี่ยวข้องกับคำขอ GET สองคำขอ คำขอแรกส่งไปยังอุปกรณ์ที่กำหนดเป้าหมายพารามิเตอร์ "get_url" ของไฟล์ PHP และคำขอที่สองสร้างขึ้นในอุปกรณ์เอง ทำให้เกิดการ injection คำสั่งที่ดำเนินการร้องขอ HTTP GET ไปยังโครงสร้างพื้นฐาน และผู้โจมตีได้ใช้ประโยชน์จากไพพ์ FIFO บนอุปกรณ์ Mitel ที่เป็นเป้าหมาย ในการส่งคำขอออกมาจากภายในเครือข่ายที่ถูกโจมตี เมื่อสร้าง reverse shell ผู้โจมตีสร้างเว็บเชลล์ (pdf_import.php) และดาวน์โหลดเครื่องมือ reverse proxy ที่เรียกว่า “Chisel” เพื่อลดโอกาสในการตรวจจับได้เมื่อเข้าไปภายในเครือข่าย

นักวิจัยด้านความปลอดภัย Kevin Beaumont กล่าวว่า มีอุปกรณ์ Mitel ที่เข้าถึงได้ทั่วไปทางออนไลน์มากกว่า 21,000 เครื่อง โดยส่วนใหญ่ตั้งอยู่ในสหรัฐอเมริกา รองลงมาคือสหราชอาณาจักร เชื่อว่าการโจมตีของแรนซัมแวร์อย่างน้อยหนึ่งครั้งจะใช้ประโยชน์จากช่องโหว่นี้ และมีแนวโน้มที่จะตามมาในไม่ช้า แนะนำให้ผู้ดูแลระบบป้องกันถึงผลกระทบโดยเร็ว

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/mitel-zero-day-used-by-hackers-in-suspected-ransomware-attack/