แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ Zero-day ในผลิตภัณฑ์ Zyxel CPE Series จำนวน 3 รายการ

วันที่แจ้งเตือน 11 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ พบว่า บริษัท Zyxel ได้ออกประกาศแจ้งเตือน กรณีการโจมตีผ่านช่องโหว่ของอุปกรณ์ Zyxel CPE Series จำนวนหลายรุ่น ซึ่งบริษัทได้ยุติการสนับสนุน (End of Support) และไม่มีการออก Patch เพื่อแก้ไขปัญหาดังกล่าวแล้ว

บริษัทรายงานช่องโหว่สำคัญของอุปกรณ์ดังกล่าวจำนวน 3 รายการ ได้แก่ CVE-2024-40890, CVE-2024-40891 และ CVE-2025-0890 ซึ่งเป็นช่องโหว่ที่เกี่ยวข้องกับการส่งคำสั่งผ่าน Telnet และมีการใช้รหัสผ่านเริ่มต้น (default password) พบว่ามีอุปกรณ์ที่ได้รับผลกระทบกว่า 1,500 เครื่อง โดยผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่เหล่านี้ เพื่อเข้าควบคุมอุปกรณ์และเข้าถึงระบบเครือข่ายได้

อุปกรณ์ Zyxel CPE Series ที่ได้รับผลกระทบ ได้แก่

VMG1312-B10A VMG1312-B10B VMG1312-B10E	VMG3312-B10A	VMG3313-B10A	VMG3926-B10B	VMG4325-B10A
VMG4380-B10A	VMG8324-B10A	VMG8924-B10A	SBG3300	SBG3500

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผู้ประกอบธุรกิจควรดำเนินการตรวจสอบอุปกรณ์ Zyxel CPE Series รุ่นที่ได้รับผลกระทบดังกล่าว วางแผนเปลี่ยนอุปกรณ์เป็นรุ่นใหม่ที่ยังได้รับการ Support จากผู้ผลิต ในระหว่างที่รอเปลี่ยนอุปกรณ์ ควรแยกอุปกรณ์ที่มีความเสี่ยงออกจากเครือข่ายหลัก จำกัดการเข้าถึงพอร์ต Telnet และบริการที่ไม่จำเป็น ทำการเปลี่ยน default password ทั้งหมดเป็นรหัสผ่านที่ซับซ้อนและปลอดภัย และเพิ่มการตรวจสอบการเข้าถึงและกิจกรรมที่ผิดปกติบนอุปกรณ์อย่างใกล้ชิด เป็นต้น

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/zyxel-wont-patch-newly-exploited-flaws-in-end-of-life-routers/
2. https://www.scworld.com/brief/actively-exploited-zyxel-router-bugs-require-immediate-model-upgrades/
3. https://techcrunch.com/2025/02/05/router-maker-zyxel-tells-customers-to-replace-vulnerable-hardware-exploited-by-hackers/
4. https://nvd.nist.gov/vuln/detail/CVE-2025-0890