แจ้งเตือน : ช่องโหว่

Alert

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

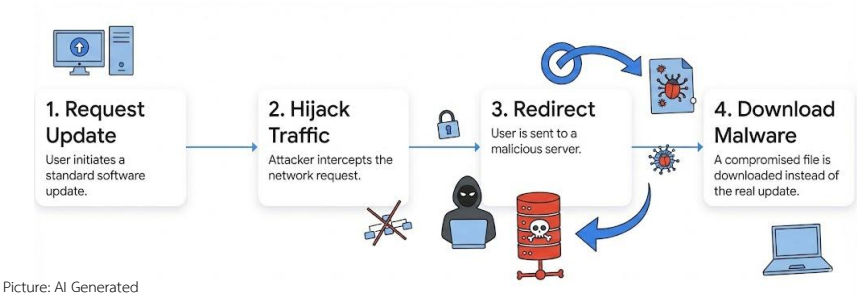
แจ้งเตือนภัยคุกคามทางไซเบอร์ของผลิตภัณฑ์ Notepad ++

วันที่แจ้งเตือน 11 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานภัยคุกคามทางไซเบอร์กรณีผู้ไม่หวังดีแทรกแซงและเปลี่ยนเส้นทางการอัปเดตซอฟต์แวร์ Notepad++ ไปยังเซิร์ฟเวอร์ที่เป็นอันตราย

กรณีดังกล่าวเกิดจากผู้ไม่หวังดีได้เจาะระบบโครงสร้างพื้นฐานของผู้ให้บริการโฮสติ้งรายเดิมของบริษัท (ระหว่างเดือนมิถุนายน ถึง ธันวาคม 2568) และได้ลักลอบเปลี่ยนเส้นทางการอัปเดตข้อมูลระบบ WinGup (Traffic Hijacking) ระหว่างผู้ใช้งานไปยังเซิร์ฟเวอร์อันตรายของผู้ไม่หวังดี ส่งผลให้มีการดาวน์โหลดไฟล์อัปเดตที่เป็นอันตราย (Compromised executables) ติดตั้งในเครื่องผู้ใช้งาน



Picture: AI Generated

ผลิตภัณฑ์	เวอร์ชันที่ได้รับผลกระทบ	เวอร์ชันที่แก้ไขแล้ว
Notepad++	Notepad++ ที่มีการอัปเดตผ่านระบบ WinGUp ในช่วงเวลาที่โครงสร้างพื้นฐานถูกแทรกแซง	v8.9.1 หรือ สูงกว่า

แนวทางการป้องกัน:
- อัปเดต Notepad++ เป็นเวอร์ชันล่าสุดตามที่แนะนำ
- ตรวจสอบความถูกต้องของไฟล์อัปเดตก่อนติดตั้ง
- สแกนระบบแบบ Full Scan หลังอัปเดตเสร็จ
- ดำเนินการตรวจสอบตัวบ่งชี้การถูกโจมตี (Indicators of Compromise: IoCs) เพื่อเฝ้าระวังกรณีเหตุการณ์ดังกล่าวได้ที่ https://dg.th/qhvy6akx7n และ https://dg.th/179j0i2ncd

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 ก.พ. 2569
2) https://notepad-plus-plus.org/news/clarification-security-incident/
3) https://notepad-plus-plus.org/news/hijacked-incident-info-update/
4) https://thehackernews.com/2026/02/notepad-official-update-mechanism.html