แจ้งเตือน

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ระดับวิกฤตใน Juniper Session Smart Routers และช่องโหว่ระดับร้ายแรงใน Winzip

วันที่แจ้งเตือน 21 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามเกี่ยวกับการโจมตีทางไซเบอร์ โดยพบว่า

1. Juniper Networks ได้เผยแพร่รายงานเกี่ยวกับช่องโหว่ในผลิตภัณฑ์ Juniper Session Smart Routers (CVE-2025-21589) ซึ่งเป็นช่องโหว่ประเภท Authentication Bypass ที่อาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมอุปกรณ์เป้าหมายในระดับ Administrator ต่ออุปกรณ์ Session Smart Router (Software-based), Session Smart Conductor และ WAN Assurance Managed Router รวมทั้ง สามารถควบคุมการรับ-ส่งข้อมูลในเครือข่ายได้ ทั้งนี้ เพื่อเป็นการลดความเสี่ยงและป้องกันผลกระทบที่อาจเกิดขึ้น องค์กรควรพิจารณาดำเนินการอัปเดตจากเวอร์ชันก่อนหน้า เป็นเวอร์ชัน 5.6.17, 6.1.12-lts, 6.2.8-lts และ 6.3.3-r2 รวมทั้ง ทำการตรวจสอบและปรับปรุงการตั้งค่าความปลอดภัยของอุปกรณ์ทั้งหมดในเครือข่าย เปลี่ยนรหัสผ่านที่เป็นค่าเริ่มต้นของระบบ และจำกัดการเข้าถึงอุปกรณ์จากภายนอกเครือข่ายอย่างเข้มงวด

2. พบช่องโหว่ร้ายแรงใน WinZip (CVE-2025-1240) ที่มีการประมวลผลไฟล์ 7Z ผิดพลาด ทำให้เกิด buffer overflow ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถเรียกใช้โค้ดที่เป็นอันตรายจากระยะไกล (Remote Code Execution (RCE)) บนคอมพิวเตอร์ที่ใช้ WinZip เวอร์ชันเก่าได้ โดยวิธีการส่งอีเมลหลอกลวง (Phishing Email) หรือสร้างโฆษณาออนไลน์ที่น่าสนใจเพื่อล่อลวงให้ผู้ใช้เปิดไฟล์ 7Z ที่ถูกสร้างขึ้นมา เพื่อการโจมตีโดยเฉพาะ หรือหลอกให้คลิกเข้าชมเว็บไซต์ที่มีการซ่อนไฟล์อันตรายไว้ เมื่อการโจมตีสำเร็จ ผู้ไม่ประสงค์ดีจะสามารถเข้าถึงและควบคุมระบบคอมพิวเตอร์ ติดตั้งโปรแกรมที่เป็นอันตราย เช่น มัลแวร์หรือแรนซัมแวร์ และอาจใช้เครื่องคอมพิวเตอร์ที่ถูกบุกรุกไปใช้เป็นส่วนหนึ่งของเครือข่ายบ็อตเน็ตสำหรับการโจมตีระบบอื่นต่อไป ทั้งนี้ เพื่อป้องกันการถูกโจมตี องค์กรควรพิจารณาดำเนินการอัปเดตโปรแกรม WinZip เป็นเวอร์ชัน 29.0 ตรวจสอบและจำกัดการใช้งานโปรแกรมดังกล่าวภายในองค์กร รวมทั้ง ควรจัดฝึกอบรมให้พนักงานตระหนักถึงความเสี่ยงและระมัดระวังในการเปิดไฟล์แนบหรือดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ ตรวจสอบ Log และตรวจสอบอีเมลที่น่าสงสัย รวมถึงปรับปรุงระบบป้องกันการเข้าถึงเว็บไซต์อันตรายให้มีประสิทธิภาพมากขึ้น

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

ข้อมูลอ้างอิง

1. https://vulnera.com/newswire/critical-remote-code-execution-vulnerability-identified-in-winzip-cve-2025-1240/
2. https://github.com/advisories/GHSA-g42f-c6cx-89cg
3. https://www.securityweek.com/critical-vulnerability-patched-in-juniper-session-smart-router/
4. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-018