แจ้งเตือน Alert	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : CLEAR
	☒ Financial Damage ☒ Reputation Damage ☒ Non-compliance ☒ Privacy Violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน เจ้าของผลิตภัณฑ์ WinRAR ออก Security Patch แก้ไขช่องโหว่ (CVE-2025-8088)

วันที่แจ้งเตือน 13 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงาน ก.ล.ต. ร่วมกับ TCM-CERT ได้ติดตามข่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์พบช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ WinRAR ที่ใช้สำหรับบีบอัดและจัดการไฟล์ (CVE-2025-8088) โดยช่องโหว่ดังกล่าวอาศัยการเรียกใช้งานโค้ดอันตรายที่ถูกจัดเก็บไว้ในไฟล์บีบอัด (special crafted archive file) เมื่อผู้ใช้งานทำการแตกไฟล์ (extract) จะทำให้โค้ดอันตรายดังกล่าวทำงาน ทำให้เกิดความเสี่ยงที่ผู้ไม่หวังดีอาจขโมยข้อมูล เข้ารหัสไฟล์เพื่อเรียกค่าไถ่ (ransomware) หรือการควบคุมระบบจากระยะไกล ซึ่งมีลักษณะคล้ายกับช่องโหว่ (CVE-2025-6218) ที่สำนักงานได้แจ้งเตือนไปเมื่อวันที่ 30 มิถุนายน 2568

RARLAB บริษัทเจ้าของผลิตภัณฑ์ WinRAR ได้ออกคำแนะนำให้ผู้ใชงานทำการอัปเดตซอฟตแวร์ตามที่แนะนำโดยเร็วที่สุด

Product Name	Affected Version	Solution
WinRAR	WinRAR, Windows versions of RAR, UnRAR, portable UnRAR source code and UnRAR.dll เวอร์ชันก่อน version 7.13	Upgrade to version 7.13

ตัวบ่งชี้การโจมตี (IOCs) ที่เกี่ยวข้อง ดังตาราง

SHA-1	Filename
371A5B8BA86FBCAB80D4E0087D2AA0D8FFDDC70B	Adverse_Effect_Medical_Records_2025.rar
D43F49E6A586658B5422EDC647075FFD405D6741	cv_submission.rar
F77DBA76010A9988C9CEB8E420C96AEBC071B889	Eli_Rosenfeld_CV2 - Copy (10).rar
676086860055F6591FED303B4799C725F8466CF4	Datos adjuntos sin título 00170.dat
1F25E062E8E9A4F1792C3EAC6462694410F0F1CA	JobDocs_July2025.rar
C340625C779911165E3983C77FD60855A2575275	cv_submission.rar
C94A6BD6EC88385E4E831B208FED2FA6FAED6666	Recruitment_Dossier_July_2025.rar
01D32FE88ECDEA2B934A00805E138034BF85BF83	install_module_x64.dll
AE687BEF963CB30A3788E34CC18046F54C41FFBA	msedge.dll
AB79081D0E26EA278D3D45DA247335A545D0512E	Complaint.exe
1AEA26A2E2A7711F89D06165E676E11769E2FD68	ApbxHelper.exe
IP	**Domain**
162.19.175[.]44	gohazeldale[.]com
194.36.209[.]127	srlaptop[.]com
85.158.108[.]62	melamorri[.]com
185.173.235[.]134	campanole[.]com

ข้อแนะนำด้านการรักษาความมั่นคงปลอดภัยที่หน่วยงานท่านอาจพิจารณาดำเนินการ

- ลบไฟล์ที่น่าสงสัยใน Startup folders และ %TEMP% หรือ %LOCALAPPDATA% (โดยเฉพาะไฟล์ .lnk หรือ .dll)
- เพิ่มการตรวจสอบอีเมลที่แนบไฟล์ RAR และให้ความรู้ผู้ใช้งานเกี่ยวกับเทคนิค “Phishing”
- พิจารณาทดสอบใน sandbox หรือ VM ก่อน extract ไฟล์ที่ได้รับทางอีเมล โดยเฉพาะจากแหล่งที่ไม่น่าเชื่อถือ
- ใช้ endpoint monitoring เพื่อตรวจจับพฤติกรรมการเขียนไฟล์และสร้าง registry สำหรับ persistence

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

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/security/winrar-zero-day-flaw-exploited-by-romcom-hackers-in-phishing-attacks/
2) https://nvd.nist.gov/vuln/detail/CVE-2025-8088
3) https://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=283&cHash=a64b4a8f662d3639dec8d65f47bc93c5
4) https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/#iocs