เอกสารการแจ้งเตือนกรณี Microsoft ออกอัปเดตแก้ไขช่องโหว่ Zero-Day ที่ส่งผลกระทบต่อ Driver Windows CLFS

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Microsoft ออกอัปเดตแก้ไขช่องโหว่ Zero-Day ที่ส่งผลกระทบต่อ Driver Windows CLFS

Microsoft ออกอัปเดตความปลอดภัยช่องโหว่หมายเลข CVE-2025-29824 ที่ส่งผลกระทบต่อ Driver Windows Common Log File System (CLFS) มีคะแนน CVSS: 7.8 ซึ่งเป็นช่องโหว่ประเภท Use-After-Free โดยสามารถถูกใช้ในการโจมตีด้วยแรนซัมแวร์ (Ransomware) หากถูกโจมตีสำเร็จ ผู้โจมตีสามารถยกระดับสิทธิ์เป็นผู้ดูแลระบบ (System Privileges) บน Windows ได้[1]

ผลิตภัณฑ์ที่ได้รับผลกระทบ

- Windows Server ทุกรุ่นถึงปี 2568
- Windows 10
- Windows 11

แนะนำให้ผู้ใช้งานหรือผู้ดูแลระบบตรวจสอบอุปกรณ์ว่ามีตัวบ่งชี้ความเสี่ยงหรือไม่ดังต่อไปนี้:

Indicators of Compromise

ตัวบ่งชี้	ประเภท	คำอธิบาย
C:\ProgramData\SkyPDF\PDU Drv.blf	Path	Dropped during CLFS exploit
C:\Windows\system32\dllhost.exe -do	Command line	Injected dllhost
Bcdedit / set {default} recoveryenabled no	Command line	Ransomware command
wbadmin delete catalog -quite	Command line	Ransomware command
wvtutil cl Application	Command line	Ransomware command
aaaaabbbbbbb.eastus.cloudapp.azure[.]com	Domain	Used by PipeMagic

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-033