TLP:CLEAR

เอกสารการแจ้งเตือนกรณีแรนซัมแวร์ใหม่ที่ชื่อว่า Helldown กำหนดเป้าหมายการโจมตีไปที่ระบบ VMware และ Linux

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Ransomware Helldown ใช้ประโยชน์จากช่องโหว่ Zyxel VPN เพื่อโจมตี VMware และ Linux

Helldown ได้เปิดเผยต่อสาธารณะเป็นครั้งแรกโดย Halcyon ในช่วงกลางปี 2567 ที่เน้นการโจมตีไปยังระบบ Windows และขยายเป้าหมายการโจมตีไปที่ระบบ VMware และ Linux และได้ใช้โค้ดจาก LockBit 3.0 [1] ซึ่งเป็นแรนซัมแวร์ที่มีชื่อเสียง โดยการโจมตีของแรนซัมแวร์ Helldown คือการใช้ช่องโหว่ในอุปกรณ์ VPN ของ Zyxel [2] และใช้ประโยชน์จากช่องโหว่ CVE-2024-42057 มีคะแนน CVSS 8.1 [3] เพื่อโจมตีโดยเน้นเป้าหมายไปที่ระบบ VMware และ Linux

ช่องโหว่ CVE-2024-42057 เป็นช่องโหว่ในการแทรกคำสั่งฟีเจอร์ IPSec ของ Zyxel ซึ่งอาจทำให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถยกระดับสิทธิ์ ปิดระบบความปลอดภัย และผู้โจมตีสามารถเรียกใช้คำสั่ง Operating System (OS) ที่สร้างขึ้นเองได้ อย่างไรก็ตามการโจมตีนี้จะสำเร็จได้ก็ต่อเมื่ออุปกรณ์ได้รับการกำหนดค่าในโหมดการตรวจสอบสิทธิ์ User-Based-PSK และผู้ใช้ต้องมีชื่อผู้ใช้ยาวเกิน 28 อักขระ [4]

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

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

อ้างอิง

1. https://thehackernews.com/2024/11/new-helldown-ransomware-expands-attacks.html
2. https://www.neowin.net/news/helldown-ransomware-attacks-expand-to-linux-and-vmware/#google_vignette
3. https://nvd.nist.gov/vuln/detail/cve-2024-42057
4. https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-