เอกสารการแจ้งเตือนกรณี Cisco ออกอัปเดตเพื่อแก้ไขช่องโหว่ระดับ Critical ใน Cisco Ultra-Reliable Wireless Backhaul (URWB)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี Cisco ออกอัปเดตเพื่อแก้ไขช่องโหว่ระดับ Critical ใน Cisco Ultra-Reliable Wireless Backhaul (URWB) ที่หมายเลข CVE-2024-20418 มีคะแนน (CVSS : 10.0) ซึ่งอาจทำให้ผู้โจมตีที่ไม่ได้รับการตรวจสอบสิทธิ์สามารถโจมตีด้วย Command Injection ด้วยสิทธิ์ root บนระบบปฏิบัติการของอุปกรณ์ที่ได้รับผลกระทบช่องโหว่ดังกล่าวเกิดจาก improper valuation ในอินเทอร์เฟซการจัดการบนเว็บ ที่ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นี้ได้โดยการส่งคำขอ HTTP ที่สร้างขึ้นไปยังอินเทอร์เฟซการจัดการบนเว็บของระบบด้วยสิทธิ์ root บนระบบปฏิบัติการของอุปกรณ์ได้

ช่องโหว่ดังกล่าวส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้

- Catalyst IW9165D Heavy Duty Access Points
- Catalyst IW9165E Rugged Access Points and Wireless Clients
- Catalyst IW9167E Heavy Duty Access Points

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้ และผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบ กิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2024-20418
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs