TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Fortinet ออกอัปเดตแก้ไขช่องโหว่ ที่ส่งผลกระทบต่อ FortiSwitch GUI

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Fortinet ออกอัปเดตแก้ไขช่องโหว่ ที่ส่งผลกระทบต่อ FortiSwitch GUI

Fortinet ออกอัปเดตเพื่อแก้ไขช่องโหว่ ที่หมายเลข CVE-2024-48887 มีคะแนน CVSS 9.3 ส่งผลกระทบต่ออินเทอร์เฟซแบบกราฟิกบนเว็บ (GUI) ของอุปกรณ์ FortiSwitch โดยช่องโหว่นี้เปิดโอกาสให้ผู้โจมตีระยะไกล สามารถส่งคำขอ HTTP ที่ถูกสร้างขึ้นมาเฉพาะ เพื่อหลบเลี่ยงกระบวนการตรวจสอบสิทธิ์ และเปลี่ยนรหัสผ่านของผู้ดูแลระบบได้โดยไม่ต้องยืนยันตัวตน หากผู้โจมตีสามารถเข้าถึงระบบได้สำเร็จ ผู้โจมตีอาจดำเนินการเปลี่ยนแปลงรหัสผ่านของผู้ดูแลระบบ และตั้งค่าระบบโดยไม่ได้รับอนุญาต รวมถึงเคลื่อนย้ายภายในเครือข่ายองค์กร เพื่อขยายขอบเขตของการโจมตีไปยังระบบหรืออุปกรณ์อื่น ๆ[1]

เวอร์ชันของ FortiSwitch ที่ได้รับผลกระทบมีดังต่อไปนี้

- FortiSwitch เวอร์ชัน 7.6.0
- FortiSwitch เวอร์ชัน 7.4.0 ถึง 7.4.4
- FortiSwitch เวอร์ชัน 7.2.0 ถึง 7.2.8
- FortiSwitch เวอร์ชัน 7.0.0 ถึง 7.0.10
- FortiSwitch เวอร์ชัน 6.4.0 ถึง 6.4.14

Fortinet แนะนำให้ผู้ใช้งานและผู้ดูแลระบบเร่งดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุด เพื่อปิดช่องโหว่ดังกล่าว หากยังไม่สามารถติดตั้งแพตช์ได้ทันที ควรใช้มาตรการป้องกันชั่วคราวเพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้น โดยมีแนวทางดังนี้

- ปิดการเข้าถึงอินเทอร์เฟซการจัดการผ่าน HTTP/HTTPS
- เปิดใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย (MFA) หากระบบรองรับ
- ตรวจสอบบันทึก (Logs) สำหรับกิจกรรมต้องสงสัย เช่น การเปลี่ยนรหัสผ่านหรือการเข้าถึง GUI
- เฝ้าระวังการรับส่งข้อมูล HTTP ที่ผิดปกติซึ่งมุ่งเป้าไปยังอินเทอร์เฟซของ FortiSwitch
- จำกัดการเข้าถึงระบบจากเฉพาะเครื่องหรือเครือข่ายที่เชื่อถือได้

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-2025-034

TLP:CLEAR