เอกสารการแจ้งเตือนกรณี Fotinet ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ระดับ Critical ใน FortiManager

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-47575 มีคะแนน (CVSS : 9.8) ใน FortiManager หากมีการใช้ประโยชน์จากช่องโหว่ได้สำเร็จอาจทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันสามารถส่งคำขอที่สร้างขึ้นเป็นพิเศษเพื่อเรียกใช้โค้ดหรือคำสั่งใด ๆ ได้จากระยะไกล[1]

ช่องโหว่ส่งผลต่อเวอร์ชันของผลิตภัณฑ์ต่อไปนี้ [2]

- FortiManager เวอร์ชัน 7.6.0
- FortiManager เวอร์ชัน 7.4.0 ถึง 7.4.4
- FortiManager เวอร์ชัน 7.2.0 ถึง 7.2.7
- FortiManager เวอร์ชัน 7.0.0 ถึง 7.0.12
- FortiManager เวอร์ชัน 6.4.0 ถึง 6.4.14
- FortiManager เวอร์ชัน 6.2.0 ถึง 6.2.12
- FortiManager Cloud เวอร์ชัน 7.4.1 ถึง 7.4.4
- FortiManager Cloud เวอร์ชัน 7.2.1 ถึง 7.2.7
- FortiManager Cloud เวอร์ชัน 7.0.1 ถึง 7.0.12
- FortiManager Cloud เวอร์ชัน 6.4.x

ผู้ดูแลระบบอาจสามารถสแกนหา Indicators of Compromise (IOC) ที่เกี่ยวข้องกับการโจมตีจากช่องโหว่ดังกล่าว

Type of IOC	IOC
Log Entry	type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="device,...",msg="Unregistered device localhost add succeeded" device="localhost" adom="FortiManager" session_id=0 operation="Add device" performed_on="localhost" changes="Unregistered device localhost add succeeded"
Log Entry	type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,at, notice,level",user="System",userfrom="",msg=""adom="root"session_id=0 operation="Modify device" performed_on="localhost" changes="Edited device settings (SN FMG-VMTM23017412)"
IP Address	45[.]32[.]41[.]202
IP Address	104[.]238[.]141[.]143
IP Address	158[.]247[.]199[.]37
IP Address	45[.]32[.]63[.]2
Serial Number	FMG-VMTM23017412
File	/tmp/.tm

File	/var/tmp/.tm

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที 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://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-134