

- Financial Damage
- Reputation Damage
- Non-compliance
- Privacy Violation

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability



แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ FortiSIEM (CVE-2024-23108 และ CVE-2024-23109)

วันที่แจ้งเตือน 4 มิถุนายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการธุรกิจหลักทรัพย์และผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล ทุกแห่ง

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Fortinet FortiSIEM จำนวน 2 รายการ ได้แก่ CVE-2024-23108 และ CVE-2024-23109 โดยช่องโหว่ดังกล่าวส่งผลให้ผู้ไม่หวังดีจากระยะไกลสามารถส่งคำสั่งที่สร้างขึ้นเพื่อขอเชื่อมต่อผ่าน API (crafted API requests) เข้าสู่ระบบได้โดยไม่ได้รับอนุญาต

ทั้งนี้ Fortinet ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด ดังตาราง

Product	Affected	Solution
FortiSIEM	7.1.0 through 7.1.1	upgrade to FortiSIEM version 7.1.2 or above
	7.0.0 through 7.0.2	upgrade to FortiSIEM version 7.0.3 or above
	6.7.0 through 6.7.8	upgrade to FortiSIEM version 6.7.9 or above
	6.6.0 through 6.6.3	upgrade to FortiSIEM version 6.6.4 or above
	6.5.0 through 6.5.2	upgrade to FortiSIEM version 6.5.3 or above
	6.4.0 through 6.4.2	upgrade to upcoming FortiSIEM version 7.2.0 or above

ThaiCERT แนะนำให้ผู้ใช้งานหรือผู้ดูแลระบบที่ใช้ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบควรทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกใช้ในการโจมตี และควรตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยที่ร้ายแรงในด้านอื่น ๆ หรือตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศ ของหน่วยงาน

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจเกิดต่อผู้ประกอบการในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบการทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 1 มิ.ย. 2567
- <https://www.fortiguard.com/psirt/FG-IR-23-130>
- <https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-064>
- <https://www.bleepingcomputer.com/news/security/exploit-released-for-maximum-severity-fortinet-rce-bug-patch-now/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ