TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Fortinet เตือนถึงช่องโหว่ใน FortiSIEM

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับคุกคามทางไซเบอร์ กรณีบริษัท Fortinet ออกเตือนถึงช่องโหว่ในระดับ Critical จำนวน 2 รายการใน FortiSIEM ที่หมายเลขช่องโหว่ CVE-2024-23108 และ CVE-2024-23109 คะแนน CVSS 10 ซึ่งอาจนำไปสู่การเรียกใช้โค้ดจากระยะไกลที่สามารถรันคำสั่งที่ไม่ได้รับอนุญาตผ่านคำขอ API ที่สร้างขึ้นได้ โดยผลิตภัณฑ์ที่ได้รับผลกระทบ[1] มีดังนี้

- FortiSIEM เวอร์ชัน 7.1.0 ถึง 7.1.1
- FortiSIEM เวอร์ชัน 7.0.0 ถึง 7.0.2
- FortiSIEM เวอร์ชัน 6.7.0 ถึง 6.7.8
- FortiSIEM เวอร์ชัน 6.6.0 ถึง 6.6.3
- FortiSIEM เวอร์ชัน 6.5.0 ถึง 6.5.2
- FortiSIEM เวอร์ชัน 6.4.0 ถึง 6.4.2

โดยเดือนกุมภาพันธ์ 2567 Fortinet ได้อัปเดตคำแนะนำของปี 2566 โดยมี 2 รายการในช่องโหว่ OS Command ที่ส่งผลต่อผลิตภัณฑ์ FortiSIEM หากถูกโจมตี ช่องโหว่เหล่านี้อาจทำให้ผู้โจมตีที่ไม่ได้รับการรับรองจากระยะไกลสามารถรันคำสั่งบนระบบได้ ซึ่งเชื่อมโยงกับช่องโหว่ CVE-2023-34992 คะแนน CVSS 9.8 ที่ได้รับการแก้ไขในเดือนตุลาคม 2566

สำหรับวิธีแก้ปัญหาเบื้องต้น หน่วยงานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบดังกล่าว ทาง Fortinet ได้แนะนำเกี่ยวกับวิธีการแก้ปัญหาเบื้องต้น ให้ทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ระบุและสำหรับผู้ใช้งานที่ไม่สามารถใช้แพตช์ได้ สามารถลดช่องโหว่ได้โดยการปิดใช้งาน SSL VPN เพื่อป้องกันการโจมตี[2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งานผลิตภัณฑ์ควรเฝ้าระวังและตรวจสอบการทำงานของผลิตภัณฑ์ที่ใช้งานภายในหน่วยงาน เพื่อตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้นและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://securityaffairs.com/158813/security/fortinet-addressed-two-critical-fortisiem-vulnerabilities.html
2. https://www.fortiguard.com/psirt/FG-IR-24-015