แจ้งเตือน : ช่องโหว่

Critical

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

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ FortiOS และ FortiProxy (CVE-2024-55591)

วันที่แจ้งเตือน 15 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

Fortinet บริษัทผู้ให้บริการโซลูชันด้านความปลอดภัยทางไซเบอร์ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ FortiOS และ FortiProxy (CVE-2024-55591) ที่อาจส่งผลให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบได้โดยไม่ต้องผ่านการยืนยันตัวตน (Authentication Bypass) และสามารถครอบครองสิทธิระดับผู้ดูแลระบบ (super-admin) ด้วยการส่งคำสั่งไปยัง Node.js WebSocket module ของผลิตภัณฑ์ที่ได้รับผลกระทบ โดยพบว่ามีการใช้ประโยชน์จากช่องโหว่ดังกล่าวในการโจมตีแล้ว

ทั้งนี้ Fortinet ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัพเดตซอฟตแวรเปนเวอรชันตามที่แนะนำโดยเร็วที่สุด ดังตาราง และ ตัวบ่งชี้ช่องโหว่ (Indicator of Compromise: IOCs) ตามอ้างอิง[1]

Version	Affected	Solution
FortiOS 7.0	7.0.0 through 7.0.16	Upgrade to 7.0.17 or above
FortiProxy 7.0	7.0.0 through 7.0.19	Upgrade to 7.0.20 or above
FortiProxy 7.2	7.2.0 through 7.2.12	Upgrade to 7.2.13 or above

สำหรับผู้ใช้งานที่ไม่สามารถติดตั้งซอฟต์แวร์เป็นเวอร์ชันตามคำแนะนำได้ทันที ทาง Fortinet แนะนำวิธีแก้ปัญหาเบื้องต้น (workaround) เพื่อเป็นการป้องกันภัยคุกคามที่อาจเกิดจากช่องโหว่ดังกล่าวเป็นการชั่วคราว โดย

1) ปิดการใช้งาน HTTP/HTTPS administrative interface โดยเฉพาะที่เป็น Internet-exposed

2) จำกัดการเข้าถึง administrative interface เฉพาะ IP addresses ที่กำหนด ผ่านทาง local-in policies

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) https://fortiguard.fortinet.com/psirt/FG-IR-24-535
2) https://www.bleepingcomputer.com/news/security/fortinet-warns-of-auth-bypass-zero-day-exploited-to-hijack-firewalls/
3) https://nvd.nist.gov/vuln/detail/CVE-2024-55591