แจ้งเตือน : ช่องโหว่

HIGH

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [ ] Non-compliance
- [ ] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [ ] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่ออัปเดต Patch FortiOS, FortiProxy และ FortiSwitchManager แก้ไขช่องโหว่รุนแรง CVE-2022-40684

วันที่แจ้งเตือน 12 ตุลาคม 2565

ตามที่ Fortinet ได้ออกประกาศชุดอัปเดตซอฟต์แวร์ (Patch) เพื่อแก้ไขช่องโหว่ CVE-2022-40684 (คะแนน CVSS : 9.6) โดยช่องโหว่ดังกล่าวส่งผลให้ผู้ไม่หวังดีสามารถ ข้ามการยืนยันตัวตน (bypass authentication) และเข้าถึงหน้าควบคุมของผู้ดูแลระบบ (administrative interface) ด้วยวิธีการสร้าง HTTP/HTTPS requests บนอุปกรณ์ ดังนี้

- FortiOS version 7.0.0 ถึง 7.0.6 และ 7.2.0 ถึง 7.2.1
- FortiProxy version 7.0.0 ถึง 7.0.6 และ 7.2.0
- FortiSwitchManager version 7.0.0 และ 7.2.0

นอกจากนี้ Fortinet ให้คำแนะนำเกี่ยวกับตัวบ่งชี้การถูกโจมตี (indicator of compromise) หากตรวจพบข้อมูล **user="Local_Process_Access"** บน log ของอุปกรณ์ ให้รีบติดต่อ customer support ทันที

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการติดตั้ง Patch ตามที่ Fortinet ประกาศ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและทดสอบก่อนนำไปใช้งานจริง ทั้งนี้ ในกรณีที่ไม่สามารถติดตั้ง Patch ได้โดยเร็ว ผู้ดูแลระบบควรจัดให้มีมาตรการป้องกัน (workaround) เช่น disable HTTP/HTTPS administrative interface และ จำกัดการเข้าถึง administrative interface เฉพาะจาก IP addresses ที่กำหนดเท่านั้น จนกว่าจะมีการติดตั้ง Patch ตามคำแนะนำดังกล่าว

นอกจากนี้ SANS Internet Storm Center (ISC) ได้แนะนำเพิ่มเติมว่า "หากบริษัทมีการใช้งานผลิตภัณฑ์ของ Fortinet ที่ดูแลโดยผู้ให้บริการภายนอก (Third party) แนะนำให้บริษัททำการตรวจสอบเพื่อให้แน่ใจว่าได้ทำการอัปเดตเรียบร้อยแล้ว"

ข้อมูลอ้างอิง

1) https://www.fortiguard.com/psirt/FG-IR-22-377
2) https://www.bleepingcomputer.com/news/security/fortinet-says-critical-auth-bypass-bug-is-exploited-in-attacks/
3) https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy
4) https://www.darkreading.com/vulnerabilities-threats/patch-now-fortinet-fortigate-and-fortiproxy-contain-critical-vuln