วันที่ 18 มิถุนายน 2568

พบช่องโหว่ Zero-Day ร้ายแรงใน Fortinet: ที่สามารถรันโค้ดโจมตีจากระยะไกลได้

เมื่อเร็วๆ นี้ ได้มีการเปิดเผยโค้ดตัวอย่าง (Proof-of-Concept: PoC) สำหรับช่องโหว่ความปลอดภัยร้ายแรงแบบ Zero-Day ซึ่งส่งผลกระทบต่อผลิตภัณฑ์หลายตัวของ Fortinet สร้างความวิตกกังวลอย่างมากต่อความปลอดภัยของโครงสร้างพื้นฐานเครือข่ายในระดับองค์กร

ช่องโหว่นี้คืออะไรและส่งผลกระทบอย่างไร?

ช่องโหว่นี้ถูกติดตามในรหัส CVE-2025-32756 และมีคะแนน CVSS สูงสุดที่ 9.8 ซึ่งบ่งชี้ว่าเป็นช่องโหว่ที่มีความรุนแรงสูงมาก มันเปิดทางให้ผู้โจมตีสามารถ รันคำสั่งจากระยะไกลได้โดยไม่ต้องยืนยันตัวตน (Remote Code Execution - RCE) ผ่านช่องโหว่ประเภท Stack-based buffer overflow

ปัญหานี้เกิดจากการประมวลผลพารามิเตอร์ AuthHash จาก cookie ภายใน endpoint /remote/hostcheck_validate ที่ปรากฏอยู่ในผลิตภัณฑ์ Fortinet หลายรายการ สาเหตุหลักมาจากข้อผิดพลาดในการตรวจสอบขอบเขตของข้อมูล (bounds checking) ที่ไม่เหมาะสมเมื่อต้องจัดการกับพารามิเตอร์ “enc” ทำให้ผู้โจมตีสามารถกระตุ้นเงื่อนไข overflow ได้โดยไม่จำเป็นต้องมีสิทธิ์เข้าถึงใดๆ

โค้ดตัวอย่างที่ถูกเผยแพร่ออกมาเขียนด้วยภาษา Python โดยใช้เทคนิค Buffer overflow บน Stack เพื่อรันคำสั่งจากระยะไกล โดยไม่ต้องผ่านกระบวนการยืนยันตัวตน เพียงแค่ส่ง HTTP POST ที่มีการแก้ไขค่าพารามิเตอร์ **enc** ภายในคุกกี้ AuthHash ไปยัง endpoint /remote/hostcheck_validate

```
python3 fortinet_cve_2025_32756_poc.py target_ip [-p port] [-d]
```

ผลิตภัณฑ์ที่ได้รับผลกระทบ:

ช่องโหว่นี้ส่งผลกระทบต่อผลิตภัณฑ์ Fortinet หลายตัว ได้แก่:

- FortiVoice
- FortiMail
- FortiNDR
- FortiRecorder
- FortiCamera

ช่องโหว่นี้เปิดช่องทางให้ผู้โจมตีจากภายนอกสามารถรันโค้ดหรือคำสั่งอันตรายได้ โดยการส่งคำร้อง HTTP ที่ถูกปรับแต่งพิเศษ ซึ่งอาจส่งผลให้ผู้โจมตีเข้าควบคุมอุปกรณ์ได้ทั้งหมด

Fortinet ยืนยันมีการโจมตีใช้งานจริงแล้ว!

Fortinet ได้ยืนยันว่า ช่องโหว่นี้กำลังถูกใช้โจมตีจริงในโลกออนไลน์ โดยเฉพาะอย่างยิ่งกับระบบ FortiVoice ทีมรักษาความปลอดภัยของ Fortinet ตรวจพบกิจกรรมของผู้ไม่หวังดีหลังจากการโจมตีสำเร็จ เช่น:

- การสแกนหาข้อมูลภายในเครือข่าย
- การลบ log ระบบเพื่อปกปิดร่องรอย
- การเปิดใช้งานฟังก์ชัน fcgi debug เพื่อดักจับข้อมูลการล็อกอินจากระบบหรือ SSH

รูปแบบการโจมตีที่พบนี้ บ่งชี้ว่าเป็นการเจาะระบบอย่างมีเป้าหมายและซับซ้อน ไม่ใช่แค่การโจมตีแบบสุ่ม

IP Address ของผู้โจมตีที่ตรวจพบ:

ผู้เชี่ยวชาญด้านความปลอดภัยระบุว่าไอพีที่เกี่ยวข้องกับกลุ่มผู้โจมตี ได้แก่ **198.105.127.124, 43.228.217.173, 43.228.217.82, 156.236.76.90, 218.187.69.244, 218.187.69.59** องค์กรต่างๆ ควรรีบบล็อก IP เหล่านี้ทันที และตรวจสอบว่าเคยมีการเชื่อมต่อจาก IP เหล่านี้มาก่อนหรือไม่

ไฟล์อันตรายที่ถูกฝังบนระบบที่ถูกโจมตี:

ผู้โจมตีได้วางไฟล์อันตรายไว้ในระบบเป้าหมายเพื่อคงสิทธิ์การเข้าถึงระยะยาว เช่น:

- ไฟล์หลักของมัลแวร์: /bin/wpad_ac_helper
- การแก้ไข crontab เพื่อเก็บข้อมูลสำคัญ
- ไลบรารีอันตราย: /lib/libfmlogin.so ซึ่งใช้ดักจับรหัสผ่าน SSH

นี่แสดงให้เห็นถึงกลยุทธ์ที่ซับซ้อนในการฝังตัวระยะยาว (persistence) ของผู้โจมตี

การแก้ไขและป้องกัน:

Fortinet ได้ออกแพตช์สำหรับผลิตภัณฑ์ทั้งหมดที่ได้รับผลกระทบแล้ว องค์กรควรรีบอัปเดตเป็นเวอร์ชันอย่างน้อยดังต่อไปนี้:

- FortiVoice: 7.2.1+, 7.0.7+, หรือ 6.4.11+
- FortiMail: 7.6.3+, 7.4.5+, 7.2.8+, หรือ 7.0.9+
- FortiNDR: 7.6.1+, 7.4.8+, 7.2.5+, หรือ 7.0.7+
- FortiRecorder: 7.2.4+, 7.0.6+, หรือ 6.4.6+
- FortiCamera: 2.1.4+

แนวทางป้องกันชั่วคราว:

หากยังไม่สามารถอัปเดตได้ทันที ให้ ปิดการเข้าถึงผ่าน HTTP/HTTPS บนหน้าจัดการของอุปกรณ์ แต่อย่างไรก็ตาม วิธีนี้เป็นเพียงทางแก้ชั่วคราวเท่านั้น และ ไม่ควรใช้แทนการติดตั้งแพตช์อย่างถาวร

ข้อมูลอ้างอิง

- https://cybersecuritynews.com/poc-exploit-fortinet-0-day-vulnerability/