

วันที่ 20 ตุลาคม 2569

พบมัลแวร์ PEERSTITCH ใช้ช่องโหว่ FortiOS หลบเลี่ยงการตรวจสอบความปลอดภัยของ VPN



พบกลุ่มผู้โจมตีที่คาดว่าจะเป็กลุ่มภัยคุกคามขั้นสูง ใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยใน Fortinet FortiOS เพื่อติดตั้งมัลแวร์ชนิดใหม่ที่ไม่เคยมีรายงานมาก่อนชื่อ PEERSTITCH ซึ่งทำงานอยู่ภายในหน่วยความจำของอุปกรณ์ และถูกพัฒนาขึ้นสำหรับระบบ ARM64 โดยเฉพาะ

การโจมตีครั้งนี้อาศัยช่องโหว่ CVE-2025-61624 (คะแนน CVSS 5.4) ซึ่งเป็นช่องโหว่ประเภท Path Traversal ในระบบรับคำสั่งของ FortiOS, FortiPAM, FortiProxy และ FortiSwitchManager โดยช่องโหว่นี้อาจเปิดโอกาสให้ผู้โจมตีที่มีสิทธิ์ระดับสูงสามารถเขียนหรือลบไฟล์ภายในระบบได้ตามต้องการ ผ่านการส่งคำสั่งที่มีการปรับแต่งพารามิเตอร์เป็นพิเศษ ทั้งนี้ Fortinet ได้ออกแพตช์แก้ไขช่องโหว่ดังกล่าวแล้วเมื่อเดือนเมษายน 2026

Daniel Gott และ Shawn Westfall นักวิจัยจากทีม Unit 42 ของ Palo Alto Networks เปิดเผยว่า "PEERSTITCH เป็นมัลแวร์ที่ไม่ทิ้งไฟล์ไว้บนดิสก์อย่างถาวร ไม่เปิดพอร์ตเพื่อรอรับการเชื่อมต่อ และไม่สร้างการเชื่อมต่อออกไปยังเครือข่ายภายนอกด้วยตัวเอง แต่จะอาศัยการรับส่งข้อมูลผ่านโปรเซสที่ทำงานอยู่ตามปกติบนอุปกรณ์ที่ติดมัลแวร์ ทำให้การตรวจจับด้วยระบบรักษาความปลอดภัยทั่วไป ทั้งในระดับอุปกรณ์และเครือข่ายทำได้ยากขึ้น"

บริษัทด้านความปลอดภัยไซเบอร์ระบุว่า พบการโจมตีดังกล่าวระหว่างการตรวจสอบเหตุการณ์บุกรุกเครือข่ายของผู้ให้บริการบริหารจัดการระบบโทรคมนาคมแห่งหนึ่ง ซึ่งเกิดขึ้นต่อเนื่องตั้งแต่เดือนกันยายน 2024 โดยการโจมตีหลายขั้นตอนนี้ถูกติดตามภายใต้ชื่อ CL-STA-0954 หรือ UNC5820 ซึ่งผู้โจมตีสามารถเข้าถึงระบบได้ในช่วงแรกด้วยการใช้ประโยชน์จากช่องโหว่ร้ายแรงใน Fortinet FortiManager ที่มีชื่อว่า FortiJump (CVE-2024-47575)

หลังจากเจาะเข้าสู่อุปกรณ์ได้สำเร็จ ผู้โจมตีได้ขโมยไฟล์ข้อมูลที่เกี่ยวข้องกับการตั้งค่าระบบ ข้อมูลที่เกี่ยวข้องกับการเข้ารหัส และไฟล์ฐานข้อมูล ซึ่งภายในมีข้อมูลของอุปกรณ์ FortiGate ที่อยู่ภายใต้การบริหารจัดการมากกว่า 500 เครื่อง โดยข้อมูลที่ถูกขโมยประกอบด้วย

- หมายเลข Serial Number ของอุปกรณ์ FortiManager และข้อมูลความสัมพันธ์ในการบริหารจัดการอุปกรณ์ทั้งหมดที่เชื่อมต่ออยู่
- ไฟล์การตั้งค่าระบบของอุปกรณ์ FortiGate มากกว่า 500 เครื่อง ทั้งในเครือข่ายภายในและเครือข่ายของลูกค้า
- ฐานข้อมูล SQLite ที่ใช้สำหรับบริหารจัดการอุปกรณ์จากส่วนกลาง
- รายการหมายเลข Serial Number ของอุปกรณ์ FortiGate มากกว่า 500 เครื่อง พร้อมหมายเลข Public IP Address ของแต่ละเครื่อง
- แผนผังเครือข่ายภายใน ตารางเส้นทางการรับส่งข้อมูล และการตั้งค่าการเชื่อมต่อเครือข่าย
- ข้อมูลบัญชีผู้ดูแลระบบ บัญชีผู้ใช้ภายใน และข้อมูลเข้าสู่ระบบ SSL/VPN ที่ถูกเข้ารหัสไว้
- ข้อมูลที่เกี่ยวข้องกับการเข้ารหัสและการยืนยันความน่าเชื่อถือของระบบ รวมถึงใบรับรองดิจิทัล (Public Certificates) และกุญแจเข้ารหัสส่วนตัว (Private Keys)

จากนั้นผู้โจมตีได้นำข้อมูลที่ขโมยไปใช้สำรวจเครือข่ายเพิ่มเติม สร้างช่องทางเข้าถึงระบบในระยะยาว ดักจับข้อมูลที่รับส่งผ่านเครือข่าย สร้างการเชื่อมต่อ FortiGate SSL/VPN โดยไม่ได้รับอนุญาต ติดตั้ง Backdoor เพื่อเปิดช่องทางลับสำหรับกลับเข้าสู่ระบบ และใช้ประโยชน์จากช่องโหว่อีกตัวหนึ่งคือ CVE-2025-61624 เพื่อยกระดับสิทธิ์และติดตั้งมัลแวร์ PEERSTITCH

มัลแวร์ PEERSTITCH เป็นไฟล์โปรแกรม Linux แบบ 64 บิต สำหรับสถาปัตยกรรม ARM64 ที่พัฒนาด้วยภาษา C โดยมีสคริปต์อัตโนมัติสำหรับดาวน์โหลดส่วนประกอบทั้งหมด 5 รายการจากเซิร์ฟเวอร์ภายนอกที่ IP Address 23.240.77[.]233:8085 ได้แก่

- pM.js เป็นสคริปต์สำหรับเตรียมสภาพแวดล้อมของระบบก่อนเริ่มการโจมตี และจะลบตัวเองหลังทำงานเสร็จ
- a.js (บันทึกเป็น index.js) เป็นโมดูล JavaScript Runtime ที่สร้างขึ้นด้วย Emscripten
- a.wasm (บันทึกเป็น index.wasm) เป็นโมดูล WebAssembly ที่ผ่านการคอมไพล์แล้ว
- b.js (บันทึกเป็น ipsem.js) เป็นสคริปต์สำหรับควบคุมและจัดการขั้นตอนการติดตั้งมัลแวร์
- dd (บันทึกเป็น lldprx) เป็นไฟล์โปรแกรม ARM64 ELF ที่ใช้แทรกโค้ดอันตรายเข้าไปในหน่วยความจำของโปรเซส และเป็นส่วนหลักของมัลแวร์ PEERSTITCH

ขั้นตอนหลักของการโจมตีจะเริ่มขึ้นหลังจากหน่วงเวลาการทำงานไว้ระยะหนึ่ง โดยสคริปต์ควบคุม ipsem.js จะเรียกใช้งานไฟล์ lldprx ซึ่งทำหน้าที่แทรกและแก้ไขโค้ดภายในหน่วยความจำของโปรเซสสำคัญ 2 ตัวใน FortiOS ได้แก่ /bin/miglogd และ /bin/iked

มัลแวร์จะตรวจสอบโครงสร้างหน่วยความจำของโปรเซสเป้าหมาย จากนั้นใช้เครื่องมือ ptrace เพื่อเข้าควบคุมและหยุดการทำงานของโปรเซสชั่วคราวผ่านคำสั่ง PTRACE_INTERRUPT ก่อนจะจัดสรรพื้นที่หน่วยความจำสำหรับรันโค้ดอันตราย และเปลี่ยนเส้นทางการทำงานของโปรเซสให้ไปเรียกใช้โค้ดที่ถูกแทรกเข้าไป

เป้าหมายของขั้นตอนนี้คือการสร้าง ช่องทางสื่อสารลับภายในหน่วยความจำระหว่างโปรเซสทั้งสองของ FortiOS แทนการใช้การเชื่อมต่อเครือข่ายหรือไฟล์ตามปกติ โดยอาศัยโปรเซสที่ถูกต้องของระบบเป็นตัวกลางในการสื่อสาร เพื่อช่วยหลบเลี่ยงการตรวจจับจากระบบรักษาความปลอดภัย

โดยเฉพาะโค้ดอันตรายที่ถูกแทรกเข้าไปในโปรเซส miglogd จะสามารถตรวจจับค่าที่ผู้โจมตีกำหนดไว้ภายในข้อมูลที่ไหลผ่านโปรเซส ซึ่งประกอบด้วยตัวบ่งชี้ 2 รายการ ได้แก่

- TCP Port 8550 เป็นค่าที่ฝังอยู่ภายในข้อมูลที่รับส่ง ไม่ใช่พอร์ตที่เปิดรอรับการเชื่อมต่อ
- IP Address 169.254.0.1 เป็นหมายเลข IP แบบ Link-local ที่ใช้เป็นค่าระบุรูปแบบข้อมูลสำหรับการตรวจจับ

เมื่อพบข้อมูลที่ตรงกับค่าดังกล่าว โค้ดอันตรายจะส่ง Session Token หรือหมายเลขระบุการเชื่อมต่อที่เกี่ยวข้องไปยังโปรเซส iked ซึ่งมีโค้ดอันตรายอีกส่วนหนึ่งคอยตรวจสอบหมายเลขดังกล่าวระหว่างการจัดการเชื่อมต่อ VPN ในขั้นตอนถัดไป หากพบว่าการเชื่อมต่อ VPN มีค่าที่ถูกกำหนดไว้ตรงกัน ระบบจะเปลี่ยนไปใช้ขั้นตอนการทำงานอีกเส้นทางหนึ่ง ซึ่งทำให้สามารถข้ามกระบวนการตรวจสอบความปลอดภัยตามปกติของ FortiOS ได้

กล่าวอีกนัยหนึ่งคือ ผู้โจมตีได้แทรกโค้ดอันตรายเข้าไปในโปรเซสสำคัญทั้งสองของ FortiOS เพื่อเปลี่ยนวิธีที่ระบบ VPN จัดการกับการเชื่อมต่อบางรายการ ทำให้การเชื่อมต่อที่มีเครื่องหมายระบุเฉพาะสามารถหลบเลี่ยงการตรวจสอบความปลอดภัยตามปกติได้

นอกจากการติดตั้งมัลแวร์ PEERSTITCH แล้ว ยังพบว่าผู้โจมตีสร้างช่องทางควบคุมและสั่งการจากระยะไกล (Command and Control: C2) แยกต่างหาก โดยอาศัยโมดูล Apache mod_md ที่มีอยู่ในอุปกรณ์ FortiGate เพื่อเปิดการเชื่อมต่อแบบ SSH Reverse Shell ทำให้ผู้โจมตีสามารถส่งคำสั่งกลับเข้ามาควบคุมอุปกรณ์จากระยะไกลได้

นักวิจัยระบุว่า "ผู้โจมตียังปลอมตัวเป็นระบบ FortiManager เพื่อดึงข้อมูลจากอุปกรณ์ FortiGate ที่อยู่ภายใต้การบริหารจัดการของเครื่องอื่น ๆ ในเครือข่ายเป้าหมาย ซึ่งแสดงให้เห็นว่าผู้โจมตีมีความเชี่ยวชาญเกี่ยวกับโครงสร้างอุปกรณ์ Fortinet การทำงานภายในของ FortiOS และโปรโตคอลที่ใช้บริหารจัดการอุปกรณ์ FortiOS เป็นอย่างดี"

แม้จะยังไม่มีหลักฐานยืนยันอย่างชัดเจน แต่นักวิจัยสงสัยว่าผู้โจมตีอาจใช้ประโยชน์จากช่องโหว่อื่นร่วมด้วย เช่น CVE-2024-26009 และ CVE-2024-26008 อย่างไรก็ตาม ทีม Unit 42 เน้นย้ำว่าการใช้ประโยชน์จากช่องโหว่ทั้งสองรายการจำเป็นต้องให้อุปกรณ์ลงทะเบียนใช้งาน FortiGate Cloud/FortiCloud SSO ก่อน ซึ่งอุปกรณ์ FortiGate ที่ได้รับผลกระทบจากเหตุการณ์นี้ไม่มีเครื่องใดลงทะเบียนใช้งานบริการดังกล่าว

นอกจากนี้ ยังพบว่ากลุ่ม CL-STA-0954 ใช้วิธีต่างๆ เพื่อลบล้างรอยการโจมตีและทำให้การตรวจสอบย้อนหลังทำได้ยากขึ้น ไม่
ว่าจะเป็น การหยุดสร้าง Syslog การลบ Crash Log การลบกระบวนการส่งข้อมูลบันทึกเหตุการณ์ รวมถึงการลบบัญชีผู้ดูแล
ระบบที่สร้างขึ้นโดยไม่ได้รับอนุญาต และลบ Auto-script ที่ใช้ในการโจมตีโดยอัตโนมัติหลังจากทำงานเสร็จ

ทีม Unit 42 ระบุว่า "เหตุการณ์บุกรุกครั้งนี้สะท้อนให้เห็นถึงภัยคุกคามที่เพิ่มขึ้นจากการใช้ระบบบริหารจัดการอุปกรณ์
เครือข่ายส่วนกลางเป็นช่องทางในการโจมตีระบบอื่น ๆ ที่อยู่ภายใต้การดูแล ขณะเดียวกัน การค้นพบมัลแวร์ PEERSTITCH
ยังแสดงให้เห็นว่ามัลแวร์ที่มุ่งโจมตีอุปกรณ์เครือข่ายมีความซับซ้อนและมีเทคนิคที่ก้าวหน้ามากขึ้น"

"ด้วยการออกแบบให้มัลแวร์ทำหน้าที่แทรกโค้ดเพียงครั้งเดียว โดยไม่ทิ้งไฟล์ถาวรไว้บนดิสก์ และสร้างช่องทางสื่อสารลับ
ระหว่างโปรเซสภายในหน่วยความจำ ผู้โจมตีจึงสามารถรักษาช่องทางเข้าถึงระบบไว้ได้อย่างต่อเนื่อง พร้อมทั้งหลบเลี่ยงการ
ตรวจจับจากระบบเฝ้าระวังความปลอดภัยแบบเดิม"

อัปเดต

เมื่อวันที่ 16 ตุลาคม 2026 สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้เพิ่มช่องโหว่
CVE-2025-61624 ลงในบัญชีช่องโหว่ที่มีการนำไปใช้โจมตีจริง หรือ Known Exploited Vulnerabilities (KEV) พร้อม
กำหนดให้หน่วยงานรัฐบาลกลางของสหรัฐฯ ดำเนินการติดตั้งแพตช์แก้ไขช่องโหว่ดังกล่าวภายในวันที่ 19 ตุลาคม 2026

ข้อมูลอ้างอิง

Oct 16, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/attackers-exploit-fortios-flaw-to.html>