วันที่ 18 มิถุนายน 2569

ผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ 3 รายการใน Fortinet FortiSandbox

Defused Cyber บริษัทด้านข่าวกรองภัยคุกคาม ได้ออกมาเปิดเผยผ่านแพลตฟอร์ม X ว่า ในช่วง 24 ชั่วโมงที่ผ่านมา ตรวจพบกลุ่มแฮกเกอร์กำลังพยายามเจาะระบบโดยอาศัยช่องโหว่ความปลอดภัยระดับร้ายแรงหลายรายการบน **Fortinet FortiSandbox** ได้แก่ CVE-2026-39813, CVE-2026-39808 และ CVE-2026-25089

- **CVE-2026-39813 (คะแนน CVSS: 9.1):** เป็นช่องโหว่ประเภท Path Traversal ที่ซ่อนอยู่ใน JRPC API ของ FortiSandbox ช่องโหว่นี้เปิดโอกาสให้แฮกเกอร์สามารถข้ามผ่านระบบยืนยันตัวตน (Authentication Bypass) ได้สำเร็จ เพียงแค่ส่งคำขอ HTTP ที่ถูกปรับแต่งมาเป็นพิเศษ
- **CVE-2026-39808 (คะแนน CVSS: 9.1):** เป็นช่องโหว่ประเภท OS Command Injection ซึ่งช่วยให้ผู้โจมตีที่ยังไม่ผ่านการยืนยันตัวตน สามารถรันโค้ดหรือป้อนคำสั่งอันตรายเข้าสู่ระบบได้ผ่านคำขอ HTTP แบบพิเศษเช่นกัน (ทั้งสองช่องโหว่นี้ทาง Fortinet ได้ปล่อยแพตช์แก้ไขไปแล้วตั้งแต่เดือนเมษายน 2026)
- **CVE-2026-25089 (คะแนน CVSS: 9.1):** เพิ่งได้รับการแก้ไขเมื่อสัปดาห์ที่ผ่านมา โดยเป็นช่องโหว่ OS Command Injection ที่กระทบทั้ง FortiSandbox, FortiSandbox Cloud และ FortiSandbox PaaS WEB UI ทำให้ผู้โจมตีที่ไม่มีสิทธิ์สามารถรันคำสั่งอันตรายได้ผ่านคำขอ HTTP

ทาง Defused Cyber ระบุจุดที่น่าสนใจว่า โค้ดสำหรับใช้โจมตี (Exploit) ช่องโหว่ CVE-2026-25089 นั้น มีลักษณะที่บ่งชี้ว่าอาจถูกเขียนขึ้นโดยใช้ปัญญาประดิษฐ์ (AI) เข้ามาช่วย อย่างไรก็ตาม โค้ดดังกล่าวยังมีข้อบกพร่องอยู่บ้าง และปัจจุบันยังไม่มีการนำโค้ดโจมตีที่ใช้งานได้จริงออกเผยแพร่สู่สาธารณะ

อุปกรณ์ของ Fortinet ตกเป็นเป้าหมายยอดฮิตของผู้โจมตีมาอย่างต่อเนื่อง ย้อนไปเมื่อเดือนเมษายน 2026 ทาง Fortinet ก็เพิ่งต้องออกแพตช์ฉุกเฉิน (Out-of-Band Patch) เพื่ออุดช่องโหว่ร้ายแรงบน FortiClient EMS (CVE-2026-35616, CVSS: 9.1) หลังจากพบว่าช่องโหว่ดังกล่าวถูกนำไปใช้โจมตีในสภาพแวดล้อมจริงแล้ว

แคมเปญ "FortiBleed" เจาะระบบ Fortinet Firewall ทะลุ 30,000 เครื่องทั่วโลก

การรายงานถึงช่องโหวใหม่เกิดขึ้นในห้วงเวลาเดียวกับที่บริษัท SOCRadar ตรวจพบปฏิบัติการทางไซเบอร์สเกลใหญ่ชื่อว่า "FortiBleed" ซึ่งดำเนินการโดยกลุ่มแฮกเกอร์ที่คาดว่าใช้ภาษารัสเซีย ปฏิบัติการนี้สามารถเจาะเข้าถึง Fortinet Firewall ได้แล้วมากกว่า 30,000 เครื่องใน 194 ประเทศทั่วโลก หลังจากที่นักวิจัยสามารถตรวจพบเซิร์ฟเวอร์สั่งการของกลุ่มดังกล่าว

- "ในฐานข้อมูลของผู้โจมตี พบข้อมูลบัญชีผู้ใช้งานของอุปกรณ์กว่า 30,791 เครื่อง ซึ่งล้วนเป็นของบริษัทเอกชนและหน่วยงานรัฐใน 194 ประเทศ" SOCRadar ระบุ
- "ที่น่ากังวลคือ ข้อมูลเหล่านี้ไม่ใช่ผลจากการสุ่มเดารหัสผ่าน แต่เป็นชื่อผู้ใช้และรหัสผ่านที่ใช้งานได้จริง ซึ่งผ่านการทดสอบและยืนยันผลโดยเครื่องมืออัตโนมัติของแฮกเกอร์ที่รันอยู่ตลอด 24 ชั่วโมง"

เป้าหมายที่ถูกเจาะระบบครอบคลุมโครงสร้างพื้นฐานสำคัญ ทั้งธนาคาร, ผู้ให้บริการโทรคมนาคม, โรงพยาบาล, มหาวิทยาลัย, บริษัทพลังงาน, องค์กรข้ามชาติ รวมถึงหน่วยงานภาครัฐ โดย 10 ประเทศที่ตกเป็นเหยื่อมากที่สุด ได้แก่ อินเดีย, สหรัฐอเมริกา, เม็กซิโก, โคลอมเบีย, ไทย, ไต้หวัน, อินโดนีเซีย, มาเลเซีย, สิงคโปร์ และฝรั่งเศส (เฉพาะในกลุ่มหน่วยงานภาครัฐ อินเดียครองสัดส่วนถึง 60% ของอุปกรณ์ Fortinet ที่เชื่อมต่ออินเทอร์เน็ตสาธารณะ)

รูปแบบการโจมตีของกลุ่มนี้ แบ่งออกเป็น 2 ขั้นตอนหลักอย่างแยบยล:

1. **เจาะด้วยรหัสผ่านเก่า:** พวกเขาเริ่มต้นด้วยการนำฐานข้อมูลรหัสผ่าน Fortinet ที่เคยรั่วไหลในอดีต ไปทดลองล็อกอินกับอุปกรณ์เป้าหมาย เนื่องจากองค์กรหลายแห่งละเลยที่จะเปลี่ยนรหัสผ่านหลังเกิดเหตุข้อมูลหลุด
2. **ดักฟังเพื่อขยายผล:** เมื่อแฮกเกอร์เจาะเข้าอุปกรณ์ได้สำเร็จ จะทำการฝังตัวเพื่อเฝ้าดักฟังทราฟฟิกเครือข่ายแบบเงียบๆ เพื่อรวบรวมข้อมูลบัญชีผู้ใช้ใหม่ๆ ที่วิ่งผ่านระบบ ก่อนจะนำไปใช้เจาะเข้าระบบอื่นๆ ต่อไปเป็นทอดๆ

ข้อมูลเจาะลึก: สเกลการโจมตีมหาศาลและการถอดรหัสผ่าน GPU

ข้อมูลเพิ่มเติมจากบริษัท Hudson Rock เมื่อวันที่ 17 มิถุนายน 2026 เผยให้เห็นขอบเขตความเสียหายที่กว้างขึ้น โดยระบุว่าแคมเปญ FortiBleed ได้โจมตีเป้าหมายไปถึง 73,932 URL ของ Firewall ใน 194 ประเทศ ส่งผลกระทบต่อโดเมนต่างๆ รวม 21,632 โดเมน

ความเคลื่อนไหวนี้ถูกตั้งข้อสังเกตเป็นครั้งแรกโดยนักวิจัยความปลอดภัย Volodymyr "Bob" Diachenko ผ่านโพสต์บน LinkedIn เมื่อสัปดาห์ที่ผ่านมา

"นี่คือการผนึกกำลังของแฮกเกอร์รัสเซียหลายกลุ่ม เพื่อกวาดต้อนบัญชีผู้ใช้งาน Fortinet FortiGate SSL VPN ทั่วโลกในสเกลระดับมหึมา" Diachenko กล่าว "พวกเขาพยายามล็อกอินถึง 1.16 พันล้านครั้ง เล็งเป้าไปที่ FortiGate 320,777 เครื่อง และโจมตีเซิร์ฟเวอร์ Microsoft SQL อีก 163,650 เครื่อง ด้วยความพยายามกว่า 2.1 พันล้านครั้ง"

นักวิจัยประเมินว่าเป้าหมายของกลุ่มนี้ไม่ได้หยุดแค่การนำรหัสผ่านเก่ามารียูส แต่พวกเขาสามารถดักจับข้อมูลการยืนยันตัวตนของระบบ SSL-VPN แล้วนำค่าแฮช (Hash) ไปทำการถอดรหัส โดยอาศัยขุมพลังจาก GPU Cluster ถึง 45 ตัวที่ทำงานประสานกันผ่านระบบ Hashtopolis เมื่อได้รหัสผ่านมาแล้ว จะใช้เพื่อเจาะลึกเข้าไปในระบบ Active Directory ภายในองค์กร เพื่อสร้างฐานที่มั่นและคงการเข้าถึงไว้ในระยะยาว

วงจรการโจมตีของกลุ่มนี้ทำงานเป็นลูป: สแกนหาอุปกรณ์ Fortinet บนอินเทอร์เน็ต -> ล็อกอินด้วยรหัสที่รั่วไหล -> ใช้เครื่องที่ถูกแฮกเป็นจุดเฝ้าสังเกตการณ์ -> ดักจับข้อมูลชุดใหม่ -> ก่อให้เกิดการเจาะระบบต่อเนื่องเป็นลูกโซ่

ทาง Hudson Rock ทิ้งท้ายประเด็นที่น่าตกใจว่า จากฐานข้อมูลที่พบ มีรหัสผ่านจำนวนมากที่เป็น รหัสผ่านที่มีความซับซ้อนสูง (Complex Passwords) แต่ก็ยังถูกเจาะได้สำเร็จ สิ่งนี้สะท้อนให้เห็นว่า นโยบายการบังคับตั้งรหัสผ่านให้ซับซ้อนนั้น "ไร้ความหมาย" โดยสิ้นเชิง หากรหัสผ่านเหล่านั้นเคยรั่วไหลออกสู่สาธารณะในรูปแบบข้อความปกติ (Plaintext) ไปแล้ว เพราะผู้โจมตีสามารถนำรหัสที่ทราบอยู่แล้ว มาไขผ่านประตูระบบความปลอดภัยได้ทันที

ข้อมูลอ้างอิง

Jun 16, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/attackers-exploit-three-fortinet.html