วันที่ 23 มิถุนายน 2569

CISA เตือนลูกค้า Fortinet หลังเหตุการณ์ FortiBleed กระทบอุปกรณ์ FortiGate แล้วกว่า 86,644 เครื่อง

เมื่อวันพฤหัสบดีที่ผ่านมา สำนักงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้ออกประกาศเตือนอย่างเร่งด่วนให้ลูกค้าที่ใช้งานอุปกรณ์ FortiGate ของบริษัท Fortinet ดำเนินการอุดช่องโหว่ด้านความปลอดภัยทันที หลังพบว่ามีการพุ่งเป้าโจมตีอุปกรณ์ที่เปิดเชื่อมต่อกับอินเทอร์เน็ตนับพันเครื่องอย่างต่อเนื่อง

การโจมตีครั้งใหญ่นี้คาดว่าเป็นฝีมือของกลุ่มแฮกเกอร์ที่ใช้ภาษารัสเซีย โดยถูกขนานนามว่า "FortiBleed" ข้อมูล ณ วันที่ 19 มิถุนายน 2569 พบว่ามีอุปกรณ์ถูกเจาะระบบไปแล้วถึง 86,644 เครื่อง

ทางด้านบริษัทวิเคราะห์ข้อมูล SOCRadar เผยสถิติข้อมูลบัญชีผู้ใช้งานที่ถูกแฮกเกอร์เจาะไปได้ ดังนี้

- บัญชีแอดมินหรือผู้ดูแลระบบทั่วไป: 35%
- บัญชีดั้งเดิมที่ติดมากับตัวเครื่องจากโรงงาน: 28.3%
- บัญชีที่แต่ละองค์กรสร้างขึ้นมาใช้งานเอง: 36.7%

ข้อมูลจาก SOCRadar ชี้ให้เห็นชัดเจนว่ายังมีอีกหลายองค์กรที่ละเลยการเปลี่ยนชื่อผู้ใช้งานหรือรหัสผ่านที่ตั้งค่ามาจากโรงงาน ซึ่งเปรียบเสมือนการเปิดประตูทิ้งไว้ให้แฮกเกอร์เดินเข้ามาได้ง่ายๆ โดยไม่ต้องเสียเวลาสุ่มเดารหัสผ่านเลย แต่ประเด็นที่น่ากังวลที่สุดคือการที่ บัญชีที่องค์กรสร้างขึ้นมาเอง ถูกขโมยไปในสัดส่วนที่มากที่สุด เรื่องนี้สะท้อนให้เห็นว่าแฮกเกอร์ไม่ได้พุ่งเป้าแค่รหัสผ่านเดิมๆ เท่านั้น แต่ยังสามารถเจาะเข้าระบบที่องค์กรตั้งขึ้นเองได้สำเร็จ ซึ่งมักเป็นผลพวงมาจากข้อมูลรหัสผ่านที่เคยรั่วไหลไปก่อนหน้านี้แล้วไม่มีการเปลี่ยนใหม่ โดยกลุ่มอุตสาหกรรมที่โดนผลกระทบหนักที่สุดคือ ธุรกิจโทรคมนาคม หน่วยงานภาครัฐ และสถาบันการศึกษา สำหรับประเทศที่พบว่ามีข้อมูลรั่วไหลมากที่สุด ได้แก่ อินเดีย สหรัฐอเมริกา เม็กซิโก โคลอมเบีย และประเทศไทย

ผู้เชี่ยวชาญระบุว่า แฮกเกอร์ใช้วิธีกวาดสแกนอินเทอร์เน็ตเพื่อหาหน้าล็อกอินระยะไกลของ Fortinet จากนั้นจะใช้เครื่องมือพิเศษที่เขียนขึ้นมาเพื่อลองล็อกอินเข้าระบบ โดยจับคู่ชื่อผู้ใช้งานและรหัสผ่านจากฐานข้อมูลที่หลุดออกมาก่อนหน้านี้ เพื่อพยายามเจาะเข้าไปในอุปกรณ์

การโจมตีนี้ถูกตั้งโปรแกรมให้ทำงานแบบอัตโนมัติและต่อเนื่อง โดยแบ่งเป็น 2 ขั้นตอนหลัก

1. **สุ่มทดสอบรหัสผ่าน:** นำรายชื่อรหัสผ่านของ Fortinet ที่เคยหลุดมาก่อนหน้านี้ มาไล่ทดสอบกับอุปกรณ์ต่างๆ ทั่วโลก
2. **ซุ่มดักจับข้อมูล:** เมื่อเจาะเข้าไปในอุปกรณ์ได้แล้ว พวกเขาจะแฝงตัวอยู่เงียบๆ เพื่อดักเก็บข้อมูลรหัสผ่านใหม่ๆ ที่วิ่งผ่านเครือข่ายนั้น และนำไปใช้เป็นกุญแจไขเข้าสู่อุปกรณ์ตัวอื่นๆ ต่อไป

ข้อมูลรหัสผ่านทั้งหมดที่แฮกเกอร์เก็บเกี่ยวมาได้นั้นเป็นข้อมูลจริงที่พร้อมใช้งาน โดยพวกเขาจะเช็กความถูกต้องของรหัสผ่านทุกชุดก่อนที่จะนำไปรวบรวมไว้ในฐานข้อมูลบัญชีของตนเอง

บริษัทด้านความปลอดภัยไซเบอร์ Hudson Rock ชี้ว่า เหตุการณ์ครั้งนี้ส่งผลกระทบรุนแรงในระดับโลกและลุกลามไปแทบทุกแวดวงธุรกิจ โดยตอนนี้แฮกเกอร์มีฐานข้อมูลรหัสผ่านที่ใช้งานได้จริงขององค์กรระดับยักษ์ใหญ่ทั่วโลกอยู่ในมือเป็นที่เรียบร้อยแล้ว

ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร (NCSC) อธิบายเสริมว่า แคมเปญ FortiBleed พุ่งเป้าไปที่ "ประตูหน้าบ้าน" ของเครือข่าย อย่าง Firewall และระบบ VPN ของ Fortinet ที่เปิดช่องทางออกสู่อินเทอร์เน็ต โดยใช้วิธีโจมตีรูปแบบต่างๆ เช่น:

- **Brute Force Attack:** การใช้โปรแกรมสุ่มเดารหัสผ่านไปเรื่อยๆ จนกว่าจะถูก
- **Dictionary Attack:** การเดารหัสผ่านโดยอิงจากคำศัพท์ที่คนนิยมตั้งกัน
- **Credential Stuffing:** การนำรหัสผ่านที่เคยหลุดจากเว็บอื่นมาลองใช้ล็อกอิน

คาดว่าแฮกเกอร์น่าจะฉวยโอกาสจากจุดอ่อนของระบบการเก็บรหัสผ่าน (Hashing) รุ่นเก่าของ FortiGate รวมถึงวิธีการเก็บข้อมูลรหัสผ่านในไฟล์ตั้งค่าแบบเดิมๆ เพื่อใช้เป็นช่องทางในการโจมตีแบบหว่านแหในครั้งนี้

บริษัท Arctic Wolf ให้ข้อมูลเพิ่มเติมว่า จริงๆ แล้ว Fortinet ได้อัปเดตระบบการจัดเก็บรหัสผ่านแอดมินให้ปลอดภัยยิ่งขึ้นแล้ว (เปลี่ยนจากแบบ SHA-256 มาเป็นอัลกอริทึม PBKDF2) ในซอฟต์แวร์ FortiOS เวอร์ชัน 7.2.11, 7.4.8 และ 7.6.1 แต่ปัญหาคือ หากองค์กรทำการอัปเดตระบบแล้ว แต่แอดมินยังไม่ได้ทำการล็อกอินเข้ามาใหม่ ระบบก็จะยังคงเก็บรหัสผ่านด้วยวิธีเก่าที่ไม่ปลอดภัยเท่าที่ควรอยู่ ทำให้หลายองค์กรยังคงตกอยู่ในความเสี่ยง

ทางโฆษกของ Fortinet ได้ชี้แจงผ่านเว็บไซต์ The Hacker News ว่า ข้อมูลรหัสผ่านที่ปรากฏออกมานี้น่าจะเป็นการนำข้อมูลเก่าที่เคยหลุดไปแล้วกลับมาใช้ใหม่ ผสมกับการถูกสุ่มเดารหัสผ่าน ไม่ได้เกิดจากช่องโหว่ใหม่หรือมีเหตุการณ์ใหม่ใดๆ เกิดขึ้นในปัจจุบัน

พร้อมทั้งย้ำเตือนให้องค์กรต่างๆ ดูแลความปลอดภัยขั้นพื้นฐานให้ดี เช่น หมั่นเปลี่ยนรหัสผ่านเป็นประจำ และที่สำคัญคือต้องเปิดใช้งานระบบยืนยันตัวตนแบบสองชั้น (MFA)

เพื่อเป็นการป้องกัน CISA ได้ออกคำแนะนำให้องค์กรปฏิบัติตาม ดังนี้

- ตัดการเชื่อมต่อของระบบ VPN และเซสชันของแอดมินที่กำลังค้างอยู่ทั้งหมดทันที
- เปลี่ยนรหัสผ่าน VPN และบัญชีแอดมินของ Fortinet ใหม่ทั้งหมด โดยเน้นย้ำพิเศษในส่วนที่เปิดให้คนภายนอกเข้าถึงได้
- ตั้งกฎเกณฑ์การใช้รหัสผ่านที่เดายากและมีความแข็งแรงสูง
- ตรวจสอบให้ชัวร์ว่าระบบบันทึกรหัสผ่านเป็นแบบใหม่ (PBKDF2) แล้ว และจัดการลบข้อมูลรหัสผ่านที่เก็บแบบเก่าทิ้งไป
- หมั่นตรวจสอบประวัติการใช้งาน (Log) ของระบบ Firewall, VPN และระบบยืนยันตัวตน เพื่อดูว่ามีคนแปลกหน้าแอบเข้ามาเปลี่ยนการตั้งค่าหรือมีพฤติกรรมน่าสงสัยหรือไม่
- เปิดใช้งานระบบยืนยันตัวตนแบบสองชั้น (MFA) ที่ป้องกันการโดนหลอกเอาข้อมูล (Phishing) ได้ ในทุกช่องทางที่คนภายนอกหรือแอดมินใช้เข้าระบบ
- ปิดช่องทางการเข้าถึงจากภายนอกที่ไม่จำเป็น และจำกัดสิทธิ์การเข้าถึงระบบจัดการหลังบ้านให้เหลือน้อยที่สุด

เรื่องราวของ FortiBleed ถูกเปิดเผยเป็นครั้งแรกเมื่อสัปดาห์ที่ผ่านมา หลังจากที่คุณ Volodymyr "Bob" Diachenko นักวิจัยด้านความปลอดภัย บังเอิญไปพบเซิร์ฟเวอร์ตัวหนึ่งที่เก็บฐานข้อมูลรหัสผ่านพร้อมใช้ของระบบ Firewall และ VPN นับพันเครื่องจาก 194 ประเทศทั่วโลก

SOCRadar ยังระบุเพิ่มเติมอีกว่า เซิร์ฟเวอร์ตัวดังกล่าวยังถูกแฮกเกอร์ใช้เป็นคลังสำหรับเก็บเครื่องมือและสคริปต์ที่ใช้โจมตีระบบแบบอัตโนมัติอีกด้วย

เหตุการณ์ครั้งนี้เป็นเครื่องเตือนใจชั้นดีที่แสดงให้เห็นว่า การนำรหัสผ่านกลับมาใช้ซ้ำและการบริหารจัดการรหัสผ่านที่หละหลวม สามารถกลายเป็นอาวุธร้ายให้ผู้ไม่หวังดีกลับมาทำร้ายเราได้อย่างง่ายดาย

นอกจากนี้ ยังเป็นการตอกย้ำความจริงที่ว่า อุปกรณ์ป้องกันเครือข่ายด่านหน้า (อย่าง Firewall หรือ VPN) ยังคงเป็นเป้าหมายสุดหอมหวานที่แฮกเกอร์พยายามเจาะเข้ามา เพื่อใช้เป็นสะพานทอดเข้าไปทำลายระบบภายในขององค์กร

อัปเดตล่าสุด

เมื่อวันที่ 19 มิถุนายน 2569 ทาง Fortinet ได้ออกมาชี้แจงข้อมูลเพิ่มเติมว่า แคมเปญ FortiBleed นี้น่าจะเกิดจากการที่แฮกเกอร์นำข้อมูลที่เคยรั่วไหลจากเหตุการณ์ในอดีตมาใช้วนซ้ำ (เช่น ข้อมูลจากช่องโหว่ CVE-2026-24858, CVE-2025-59718 และ CVE-2025-59719) ร่วมกับการนำไปสุ่มเดารหัสผ่านกับอุปกรณ์ที่ตั้งรหัสผ่านไว้แบบเดาง่าย และไม่ได้เปิดใช้ระบบ MFA

เพื่อเป็นการลดความเสี่ยง Fortinet ได้แนะนำให้ผู้ใช้งานรีบดำเนินการดังนี้

- สั่งปิดการทำงานของแอดมินและ VPN ที่เชื่อมต่ออยู่ทั้งหมด แล้วจัดการรีเซ็ตรหัสผ่านใหม่
- เปิดใช้งานการยืนยันตัวตนแบบสองชั้น (MFA) ทันที
- อัปเดตระบบ FortiOS ให้เป็นเวอร์ชันใหม่ล่าสุด (ในกลุ่มสาย 7.4, 7.6 หรือ 8.0)
- ตรวจสอบรายชื่อผู้ใช้งาน ระบบ Firewall หรือ VPN ว่ามีใครแปลกปลอมแอบเข้ามาเปลี่ยนการตั้งค่าหรือไม่
- หมั่นเช็กประวัติการเข้าใช้งาน (Log) เพื่อดูว่ามีแอดมินแปลกหน้าเข้ามาจากหมายเลข IP ที่ไม่รู้จักหรือไม่ คอยจับตาดูพฤติกรรมการพยายามแอบเจาะลึกเข้าไปยังระบบอื่นภายในเครือข่าย (Lateral Movement) การเข้าใช้งานในเวลาที่ผิดปกติ การแอบสร้างบัญชีผู้ใช้งานใหม่ หรือการแก้การตั้งค่าโดยพลการ
- จำกัดการเข้ามาจัดการระบบจากภายนอกให้น้อยที่สุด เช่น อนุญาตให้เข้าได้เฉพาะเครื่องคอมพิวเตอร์ที่ไว้ใจได้ (Trusted Hosts) ใช้ระบบนโยบายความปลอดภัยเฉพาะจุด (Local-In Policy) หรือวิธีที่ดีที่สุดคือ ปิดไม่ให้สามารถเข้ามาตั้งค่าระบบผ่านทางอินเทอร์เน็ตได้เลย

คุณ Carl Windsor ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ (CISO) ของ Fortinet กล่าวทิ้งท้ายว่า หากระบบขององค์กรมีการเชื่อมต่อกับฐานข้อมูลบัญชีพนักงานส่วนกลาง (อย่าง Active Directory หรือ LDAP) ขอให้ประเมินสถานการณ์ไว้ก่อนเลยว่าบัญชีเหล่านั้นอาจจะถูกเจาะไปแล้ว สิ่งที่ต้องทำคือรีบตรวจสอบว่ามีการนำบัญชีเหล่านั้นไปแอบล็อกอินที่ระบบอื่นหรือไม่ มีการแอบสร้างบัญชีแฝงเพิ่มขึ้นมาหรือเปล่า และต้องเฝ้าระวังการรุกล้ำเจาะลึกเข้ามายังระบบภายในเครือข่ายอย่างใกล้ชิดที่สุด

ข้อมูลอ้างอิง

Jun 19, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/cisa-warns-fortinet-customers-as.html