

วันที่ 9 ตุลาคม 2569

FBI เตือนแคมเปญ FortiBleed ยังคงโจมตีอย่างต่อเนื่อง หลังขโมยข้อมูลบัญชีอุปกรณ์ Fortinet ได้กว่า 86,644 รายการ



สำนักงานสอบสวนกลางสหรัฐ (FBI) และหน่วยงาน United States Secret Service (USSS) ออกคำเตือนเมื่อวันอังคารว่า แคมเปญขโมยข้อมูลบัญชีผู้ใช้ที่เรียกว่า FortiBleed ยังคงเป็นภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่อง โดยมุ่งเป้าไปยังอุปกรณ์ไฟร์วอลล์ Fortinet FortiGate และเกตเวย์เครือข่ายส่วนตัวเสมือน (VPN) ที่ใช้โปรโตคอล SSL ซึ่งเปิดให้เข้าถึงได้จากอินเทอร์เน็ต แคมเปญนี้อาศัยข้อมูลบัญชีที่ถูกนำกลับมาใช้ซ้ำหรือรั่วไหล รวมถึงการจัดเก็บรหัสผ่านแบบเก่าด้วย SHA-256 ทำให้ผู้โจมตีสามารถรวบรวมและถอดรหัสข้อมูลยืนยันตัวตนได้ในวงกว้าง จากการตรวจสอบเบื้องต้นพบว่า ผู้โจมตียังคงแสวงหาไฟร์วอลล์ Fortinet ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต โดยใช้ข้อมูลบัญชีที่เคยถูกขโมยไปก่อนหน้านี้ ทั้งสองหน่วยงานระบุ

FortiBleed ได้รับการเปิดเผยเป็นครั้งแรกโดย SOCRadar และ Hudson Rock ในเดือนมิถุนายน 2026 โดยกิจกรรมดังกล่าวมุ่งเป้าไปยังไฟร์วอลล์ Fortinet หลายพันเครื่อง ซึ่งเป็นส่วนหนึ่งของแคมเปญโจมตีทั่วโลก คาดว่าปฏิบัติการนี้ดำเนินการโดยกลุ่มที่ใช้ภาษารัสเซีย และสามารถรวบรวมข้อมูลบัญชีที่ยังใช้งานได้ของอุปกรณ์มากกว่า 86,644 รายการ จาก 194 ประเทศ ณ วันที่ 19 มิถุนายน 2026

แคมเปญดังกล่าวทำให้สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา (CISA) ออกคำแนะนำให้ลูกค้าที่ใช้อุปกรณ์ FortiGate ดำเนินมาตรการป้องกัน ได้แก่ เปิดใช้ระบบยืนยันตัวตนที่ทนทานต่อการโจมตีแบบฟิชซิง ยุติเซสชัน SSL VPN และเซสชันผู้ดูแลระบบที่กำลังใช้งานอยู่ เปลี่ยนรหัสผ่าน VPN และบัญชีผู้ดูแลระบบของ Fortinet ใช้อัลกอริทึม Password-Based Key Derivation Function 2 (PBKDF2) ในการจัดเก็บข้อมูลยืนยันตัวตนของผู้ดูแลระบบ และตรวจสอบบันทึกเหตุการณ์เพื่อค้นหากิจกรรมที่น่าสงสัย

FortiBleed เป็นแคมเปญโจมตี 5 ขั้นตอน โดยเริ่มจากการสำรวจระบบในวงกว้างเพื่อค้นหาพอร์ทัลที่เปิดให้เข้าถึงจากภายนอก จากนั้นพยายามเข้าสู่ระบบด้วยเทคนิค Credential Stuffing และ Password Spraying โดยอาศัยข้อมูลจากฐานข้อมูลที่รั่วไหลก่อนหน้านี้และบันทึกการทำงานของมัลแวร์ขโมยข้อมูล (Infostealer) เมื่อเข้าถึงอุปกรณ์ได้แล้ว ผู้โจมตีจะติดตั้งเครื่องมือที่พัฒนาด้วยภาษา Go ชื่อ FortigateSniffer เพื่อดักจับข้อมูลการยืนยันตัวตนผ่านเครือข่ายในลักษณะที่ไม่รบกวนการทำงาน โดยรองรับโปรโตคอล 24 รายการ และรวบรวมทั้งข้อมูลบัญชีผู้ใช้และค่าแฮชของรหัสผ่าน

จากนั้น ค่าแฮชของรหัสผ่านจะถูกส่งไปยังระบบถอดรหัสที่ใช้ GPU ช่วยเร่งความเร็ว โดยใช้เครื่องมือ Hashmat และ Hashtopolis เพื่อถอดรหัสแบบออฟไลน์ เมื่อได้ข้อมูลแล้ว ผู้โจมตีจะนำไปใช้ขยายการเข้าถึงไปยังระบบอื่นภายในเครือข่ายสำรวจ Active Directory ตรวจสอบข้อมูลยืนยันตัวตน Kerberos และยืนยันตัวตนผ่าน SMB ในขั้นตอนสุดท้าย ผู้โจมตีจะขโมยข้อมูลสำคัญจากพื้นที่แชร์ไฟล์ในเครือข่าย พร้อมใช้คุกกี้เซสชันที่ขโมยมาเพื่อรักษาสถานะการเข้าถึงระบบอย่างต่อเนื่อง

ข้อมูลบัญชีที่ถอดรหัสได้จะถูกนำมารวบรวม จัดเรียง และตรวจสอบความถูกต้อง โดยมีการใช้สคริปต์คัดกรองระบบ Honeypot สำรวจองค์กร และจัดลำดับความสำคัญของเป้าหมายที่มีมูลค่าสูง โดยพิจารณาจากรายได้และโครงสร้างเครือข่าย เมื่อได้ข้อมูลบัญชีที่ผ่านการตรวจสอบแล้ว ผู้โจมตีจะเจาะลึกเข้าไปในระบบของเหยื่อ สำรวจข้อมูลและโครงสร้างเครือข่าย รวมถึงใช้เทคนิค Password Spraying เพื่อขยายการเข้าถึงและค้นหาบัญชีที่มีสิทธิ์ระดับสูง

นอกจากนี้ ผู้โจมตียังใช้การเข้าถึงครั้งแรกเพื่อสร้างบัญชีใหม่บนอุปกรณ์ ซึ่งเป็นวิธีรักษาสถานะการเข้าถึงให้คงอยู่ต่อไป โดยพบชื่อบัญชีที่ถูกใช้ในการโจมตีและเชื่อมโยงกับการบุกรุกหลายรายการ ดังนี้

- adminin
- fortiAdmin
- forticloud-sync
- admin
- fgtsecure
- pakedge
- forticloud-tech
- districtadmin
- system_config
- gttadmin
- roadmin
- itadmin
- Technical_support
- adminsslvpn
- IT_Manager
- my_admin
- support_fortinet
- fgtsec
- forti_support2

คาดว่าผู้โจมตีอาจทำหน้าที่เป็นนายหน้าซื้อขายสิทธิ์เข้าถึงระบบเบื้องต้น (Initial Access Broker) โดยรวบรวมข้อมูลที่ยึดมาแล้วนำไปขายต่อให้กับกลุ่มผู้โจมตีรายอื่น หลักฐานที่สนับสนุนข้อสันนิษฐานนี้คือการพบความเชื่อมโยงด้านรูปแบบการปฏิบัติการระหว่าง FortiBleed กับปฏิบัติการแรนซัมแวร์ของกลุ่ม INC และ Lynx ซึ่งอาจบ่งชี้ว่ามีการนำสิทธิ์เข้าถึงที่ได้มาไปใช้ติดตั้งแรนซัมแวร์ จากการตอบสนองต่อเหตุการณ์ในเบื้องต้น พบว่าเหยื่อบางรายอาจสูญเสียสิทธิ์ในการเข้าถึงอุปกรณ์ Fortinet ของตนเอง หากผู้โจมตีลบบัญชีเดิมหรือเปลี่ยนรหัสผ่านของบัญชีที่มีอยู่ในระบบ" FBI และ USSS เตือน

ในระหว่างการบุกรุกครั้งแรก ผู้โจมตีจะสร้างบัญชีใหม่ที่ไม่เคยมีอยู่บนอุปกรณ์มาก่อน ในบางกรณี ผู้โจมตีจะลบบัญชีเดิมเพื่อขัดขวางไม่ให้องค์กรเข้าถึงอุปกรณ์ที่ได้รับผลกระทบ และรักษาสีทธิ์การเข้าถึงระบบไว้ระหว่างพยายามขยายการโจมตีไปยังระบบอื่นภายในเครือข่าย

หากตรวจพบสัญญาณที่บ่งชี้ว่าอุปกรณ์อาจถูกบุกรุก องค์กรควรแยกอุปกรณ์ที่ได้รับผลกระทบออกจากเครือข่าย รวบรวมหลักฐานและบันทึกเหตุการณ์ที่จำเป็น รายงานเหตุการณ์ต่อ FBI และ USSS พร้อมดำเนินการรับมือที่เหมาะสมเพื่อลดความเสี่ยงจากภัยคุกคามดังกล่าว

อัปเดตเพิ่มเติม

ในแถลงการณ์ที่ส่งให้ The Hacker News นั้น Ensar Seker ประธานเจ้าหน้าที่ฝ่ายความปลอดภัยสารสนเทศ (CISO) ของ SOCRadar กล่าวว่า คำเตือนฉบับล่าสุดช่วยยืนยันข้อประเมินของบริษัทที่ว่า "FortiBleed ควรถูกมองว่าเป็นปฏิบัติการเข้าถึงระบบที่ยังดำเนินอยู่ ไม่ใช่เพียงเหตุการณ์ข้อมูลบัญชีรั่วไหลที่เกิดขึ้นครั้งเดียวแล้วจบไป"

Seker กล่าวเพิ่มเติมว่า "การสแกนระบบอย่างต่อเนื่องด้วยข้อมูลบัญชีที่ถูกขโมยไปก่อนหน้านี้ การสร้างบัญชีผู้ดูแลระบบโดยไม่ได้รับอนุญาต และรายงานกรณีที่เกี่ยวข้องถูกตัดสิทธิ์การเข้าถึง แสดงให้เห็นว่าผู้โจมตียังคงพยายามรักษาและขยายการเข้าถึงระบบ หลักฐานที่มีอยู่สนับสนุนอย่างชัดเจนว่า ผู้โจมตียังคงตรวจสอบความถูกต้องของข้อมูลบัญชี นำข้อมูลเดิมกลับมาใช้ซ้ำ และพยายามเจาะเข้าสู่ระบบ"

นอกจากจะพบความเชื่อมโยงโดยตรงระหว่างสิทธิ์การเข้าถึงที่ได้จาก FortiBleed กับเครือข่ายปฏิบัติการของแรนซัมแวร์ INC และ Lynx แล้ว บริษัทด้านข่าวกรองภัยคุกคามแห่งนี้ยังยืนยันว่า พบการติดตั้งแรนซัมแวร์อย่างน้อย 12 เหตุการณ์ที่มีต้นทางจากการเข้าถึงระบบผ่านแคมเปญดังกล่าว ส่งผลให้เครื่องปลายทางหลายร้อยเครื่องถูกเข้ารหัสข้อมูล

การที่นายหน้าซื้อขายสิทธิ์เข้าถึงระบบเบื้องต้นซึ่งใช้วิธีโจมตีแบบ FortiBleed ส่งต่อสิทธิ์เข้าถึงให้กับเครือข่ายพันธมิตรของแรนซัมแวร์ Payload ด้วย เป็นหลักฐานที่บ่งชี้ว่าปฏิบัติการนี้มีแรงจูงใจทางการเงิน และเป็นส่วนหนึ่งของเครือข่ายการส่งต่อการโจมตีด้วยแรนซัมแวร์ในวงกว้าง ไม่ได้จำกัดอยู่กับแรนซัมแวร์เพียงกลุ่มเดียว

"ประเด็นสำคัญคือ ข้อมูลบัญชีที่รั่วไหลไม่ได้กลายเป็นข้อมูลที่ปลอดภัยเพียงเพราะเวลาผ่านไปนาน" Seker กล่าว "หากข้อมูลบัญชีนั้นยังใช้งานได้ หรือผู้โจมตีสร้างบัญชีที่ช่วยให้เข้าถึงอุปกรณ์ได้อย่างต่อเนื่องไว้แล้ว ข้อมูลเหล่านี้ก็ยังสามารถใช้เป็นช่องทางเข้าสู่ระบบได้ แม้เวลาจะผ่านไปหลายเดือนนับจากวันที่มีการขโมยข้อมูลครั้งแรก"

"ดังนั้น องค์กรควรมองความเป็นไปได้ที่ข้อมูลรั่วไหลว่าเป็นเหตุการณ์ที่ระบบอาจถูกบุกรุกแล้ว โดยจำกัดการจัดการอุปกรณ์จากภายนอก ยุติเซสชันที่กำลังใช้งาน เปลี่ยนข้อมูลยืนยันตัวตนของบัญชีผู้ดูแลระบบและ VPN ตรวจสอบบัญชีผู้ใช้ภายในระบบและบัญชี API ทั้งหมด บังคับใช้ MFA ที่ทนทานต่อการโจมตีแบบฟิชซิง และตรวจสอบกิจกรรมที่เกิดขึ้นต่อจากการเข้าถึงครั้งแรก แทนที่จะพึ่งพาการอัปเดตแพตช์เพียงอย่างเดียว"

Dray Agha ผู้จัดการอาวุโสฝ่าย Tactical Response ของ Huntress แนะนำให้องค์กรบังคับใช้การยืนยันตัวตนหลายปัจจัย (MFA) สำหรับการเข้าถึงระบบจากระยะไกลทุกช่องทาง ตรวจสอบระบบเพื่อค้นหาบัญชีที่เพิ่งถูกสร้างขึ้น และปิดอินเทอร์เฟซสำหรับการจัดการระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต

"การโจมตีอุปกรณ์ที่อยู่บริเวณขอบเครือข่าย เช่น VPN และไฟร์วอลล์ ไม่ใช่เรื่องใหม่ แต่สิ่งที่ทำให้แคมเปญ FortiBleed แตกต่างออกไปคือ ความแตกต่างระหว่างการเข้าถึงระบบครั้งแรกที่เกิดขึ้นอย่างเงียบ ๆ กับการยึดครองระบบอย่างรุนแรงที่ตามมา" Ben Bernstein ผู้จัดการทีม Cybersecurity Advisors Team ของ Huntress กล่าวในแถลงการณ์

"ผู้โจมตีกำลังขโมยไฟล์การตั้งค่าระบบ นำค่าแฮชของรหัสผ่านไปถอดรหัสมัลแวร์ออนไลน์ด้วยฮาร์ดแวร์ของตนเอง และเข้าสู่ระบบได้ตั้งแต่การลองครั้งแรก โดยไม่ทำให้เกิดการแจ้งเตือนจากการเข้าสู่ระบบล้มเหลวแม้แต่ครั้งเดียว เมื่อเข้ามาในระบบได้แล้ว พวกเขากลับไม่ทำตามแนวทางปกติของนายหน้าซื้อขายสิทธิ์เข้าถึงระบบที่มักพยายามหลีกเลี่ยงการตรวจจับ แต่กลับเปลี่ยนรหัสผ่านผู้ดูแลระบบอย่างเปิดเผย ตัดสิทธิ์ทีมไอทีที่แท้จริงไม่ให้เข้าถึงอุปกรณ์ขององค์กรเอง และส่งมอบสิทธิ์ควบคุมให้กับกลุ่มแรนซัมแวร์อย่าง INC และ Payload โดยตรง"

"เมื่อองค์กรไม่สามารถเข้าถึงไฟร์วอลล์ของตนเองได้อีกต่อไป ก็ไม่สามารถแก้ปัญหาด้วยการติดตั้งแพตช์ซอฟต์แวร์แล้วจบเรื่องได้ เพราะผู้โจมตีรู้ว่าองค์กรอาจจำเป็นต้องเข้าถึงอุปกรณ์โดยตรงเพื่อรีเซ็ตกลับเป็นค่าโรงงาน และติดตั้งระบบใหม่ทั้งหมด ก่อนที่การเข้ารหัสข้อมูลจะเริ่มต้นขึ้น"

(ข่าวนี้ได้รับการปรับปรุงหลังเผยแพร่ โดยเพิ่มเติมข้อมูลจาก SOCRadar และ Huntress)

ข้อมูลอ้างอิง

Oct 7, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/fbi-warns-fortibleed-remains-active.html>