เทรนด์ไมโคร แนะรับมือ Heartbleed ช่องโหว่บนเว็บไซต์ที่สร้างความเสี่ยงให้กับระบบเข้ารหัสข้อมูล SSL ที่ซึ่งเก็บข้อมูลทั้งหมด รวมถึงข้อมูลธุรกรรมออนไลน์ต่างๆ ของสมาชิกเว็บไซด์นั้นๆ

กรุงเทพฯ – 11 เมษายน 2557 ผู้เชี่ยวชาญของเทรนด์ไมโคร เตือนถึงช่องโหว่ Heartbleed ว่าประกอบไปด้วยระบบการเข้ารหัส SSL หลากหลายเวอร์ชั่น ซึ่งเป็นเทคโนโลยีที่ช่วยป้องกันข้อมูลทั้งหมด รวมถึงข้อมูลธุรกรรมออนไลน์ต่างๆ ของสมาชิกเว็บไซด์บนอินเทอร์เน็ต

นายคริสโตเฟอร์ บัดด์ ผู้จัดการด้านการสื่อสารภัยคุกคามระดับโลกของเทรนด์ ไมโคร กล่าวว่า “ช่องโหว่ Hearbleed นี้เป็นปัญหาที่มีผลกระทบต่อระบบเข้ารหัส SSL ที่ผู้ใช้งานออนไลน์คุ้นเคยด้วยสัญลักษณ์รูป “กุญแจล็อก” ที่ซึ่งยืนยันว่า เว็บไซด์นั้นๆ มีระบบเข้ารหัสเพื่อป้องกันข้อมูลผู้ใช้งาน โดยเฉพาะอย่างยิ่งหากมีการทำธุรกรรมออนไลน์ ช๊อปปิ้งออนไลน์ ที่มีกรอกกข้อมูลส่วนตัวต่างๆ วันเดือนปีเกิด ข้อมูลการเงิน เช่น หมายเลขบัตรเครดิต วันหมดอายุ หมายเลขพิเศษหลังบัตรเครดิต ผ่านหน้าเว็บไซต์”

หากช่องโหว่นี้เปิดกว้าง ผู้ไม่หวังดีสามารถเข้าไปยังระบบป้องกันภัยของเว็บไซต์นั้นๆ ทำให้สามารถ ติดตามการสื่อสาร ระหว่างผู้ใช้งานทั้งหมด และเว็บไซต์ รวมถึงสามารถถอดรหัสการใช้งานที่ผ่านมาบนเว็บ อาจสร้างความเสียหาย ให้กับผู้ใช้บริการทั้งหมดได้ด้วย

นายบัดด์ กล่าวเพิ่มเติมว่า “เหตุการณ์เหล่านี้หมายความว่า ข้อมูลที่มีความอ่อนไหว เช่น รหัสผ่าน ข้อมูลเกี่ยวกับบัตรเครดิต หรือข้อมูลส่วนตัว สามารถตกไปถึงผู้อื่นโดยที่คุณไม่สามารถทราบได้เลย

แล้วเราสามารถทำอะไรได้บ้างเมื่อเกิดเหตุการณ์นี้ขึ้น เราสามารถแก้ปัญหานี้ได้ด้วยตนเองไหม

นายบัดด์ กล่าวว่า “ในกรณีนี้ปัญหาไม่ได้อยู่ที่คอมพิวเตอร์ของคุณ หรืออุปกรณ์ที่คุยใช้งาน มันเป็นปัญหาที่เว็บไซต์นั้นๆ ต้องเข้ามาดูแลด้วยการแก้ไข SSL บนเว็บไซต์ของตน”

คำแนะนำเบื้องต้นสำหรับผู้ใช้งานออนไลน์ เพื่อหลีกเลี่ยงปัญหาช่องโหว่ Heartbleed

1. ตรวจสอบให้มั่นใจว่าระบบทุกระบบ ใช้ซอฟต์แวร์ป้องกันความปลอดภัยที่อัพเดทอยู่เสมอ
2. พิจารณาเปลี่ยนรหัสผ่านในบัญชีที่มีความสำคัญ เช่น เว็บเมล์ หรือระบบการเงินออนไลน์
3. ตรวจสอบกิจกรรมที่น่าสงสัยทุกชนิด โดยเฉพาะอย่างยิ่งที่เกิดจากบัญชีออนไลน์ และการเงิน
4. เปลี่ยนรหัสผ่านทันทีในทุกไซต์ที่แนะนำให้คุณเปลี่ยน

นายบัดด์ กล่าวเสริมว่า “ปัญหานี้เป็นปัญหาใหญ่ ที่สามารถขยายผลไปยังกลุ่มผู้ใช้งานจำนวนมาก และสามารถทำให้เกิดปัญหา ความปลอดภัยที่ร้ายแรงกับเว็บไซต์ และผู้ใช้งานเว็บนั้นๆ เหล่าอาชญากรออนไลน์ อาจเห็น หรือทราบข้อมูลการสื่อสาร ระหว่างเว็บไซต์ กับผู้ใช้งาน และทำการเลียนแบบเว็บไซต์ หรือพฤติกรรมผู้บริโภค เพื่อขโมยข้อมูลที่สำคัญอื่นๆ ไปได้

ติดตามรายละเอียดเพิ่มเติมได้

บทความ

- http://esupport.trendmicro.com/solution/en-US/1103084.aspx

บล็อคโพสจากผู้เชี่ยวชาญ

- http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability
- http://blog.trendmicro.com/heartbleed-vulnerability/

ท่านสามารถใช้ข้อมูลในอีเมล์ หรือบล๊อคโพสต์นี้ได้อย่างอิสระ ผู้เชี่ยวชาญจากเทรนด์ ไมโคร รวมถึง นายคริสต์โต เฟอร์ บัดด์ พร้อมที่จะพูดคุยกับท่านเกี่ยวกับภัยคุกคามนี้ ในกรณีที่ท่านสนใจข้อมูลเพิ่มเติม หรือต้องการพูดคุยกับ

ผู้เชี่ยวชาญ ด้านการป้องกันภัยคุกคามของเทรนด์ ไมโคร กรุณาแจ้งให้เราทราบ เราจะประสานงานให้ท่านทันที

เกี่ยวกับเทรนด์ ไมโคร

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะปกป้องโลกให้ปลอดภัย เพื่อรองรับการแลกเปลี่ยนข้อมูลดิจิตอล นวัตกรรมโซลูชั่นของเราให้บริการสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น (Layered content security) ในอุปกรณ์พกพา อุปกรณ์ปลายทาง เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th