The OpenSSL Heartbleed Bug Alert

"ปัญหาของ OpenSSL และแนวทางแก้ไข"

“รู้จักกับ Heartbleed Bug ก่อนที่เลือดจะไหลหมดหัวใจ”

โดย สมาคมผู้ดูแลเว็บไทย, สมาคม eCommerce, TISA, และ ACIS Cyber Lab.

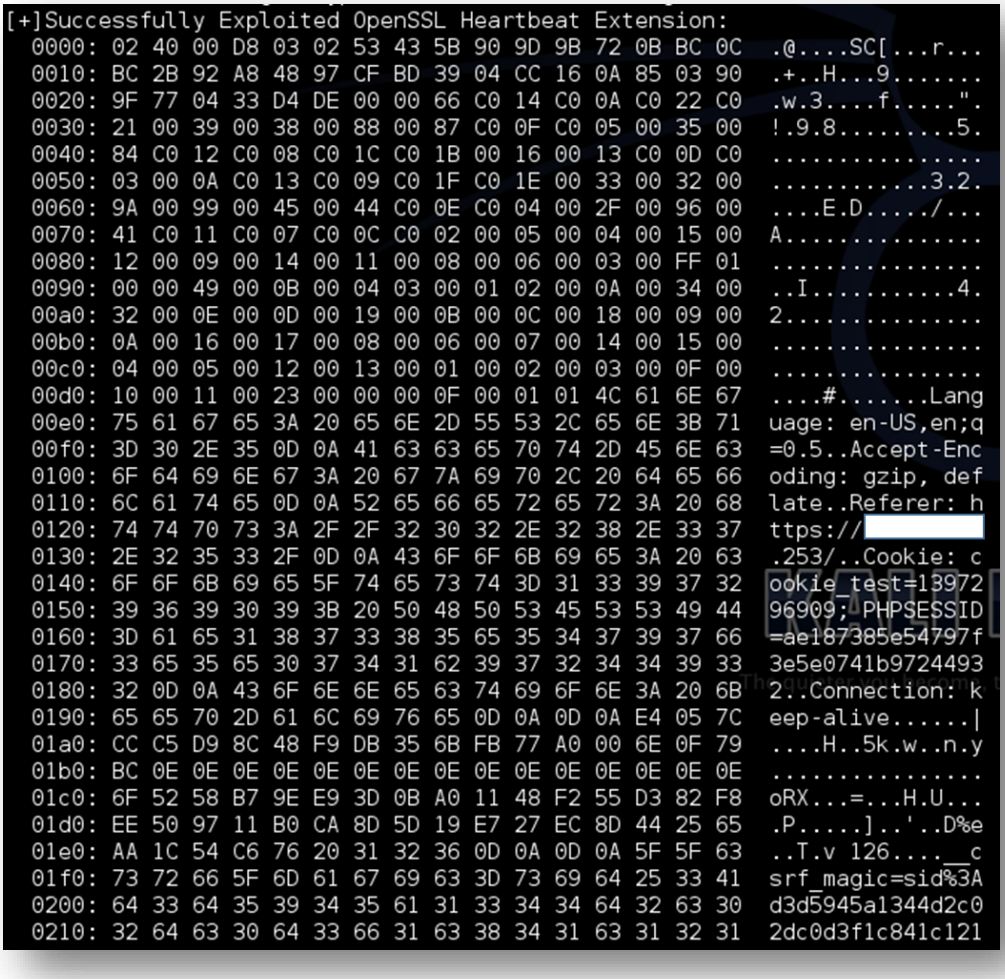
## Heartbleed Bug คืออะไร?

Heartbleed Bug เป็นช่องโหว่ความเสี่ยงสูงที่มีอยู่ใน OpenSSL Library ซึ่งเว็บไซต์นับล้านทั่วโลกใช้งาน Library นี้อยู่ โดยที่ OpenSSL Library นี้จะถูกเรียกใช้งานโดย Application ที่ต้องการเข้ารหัสการรับส่งข้อมูลโดยใช้ SSL/TLS (เช่น HTTPS, VPN, EMAIL) ผลกระทบที่เกิดจาก Heartbleed Bug คือการที่ผู้โจมตีสามารถเข้าถึงข้อมูลที่อยู่ในหน่วยความจำหลัก (หรือ RAM นั่นเอง) ได้จากระยะไกล ซึ่งเป็นที่ทราบกันดีอยู่แล้วว่าข้อมูลในระหว่างการรับ-ส่ง นั้น จะถูกเข้ารหัสโดย SSL/TLS แต่เมื่อข้อมูลถูกส่งมาถึงผู้รับและเข้าไปอยู่ใน RAM นั้นจะเป็น plaintext หรือพูดง่าย ๆ ว่า ไม่ได้ถูกเข้ารหัสแล้วนั่นเอง

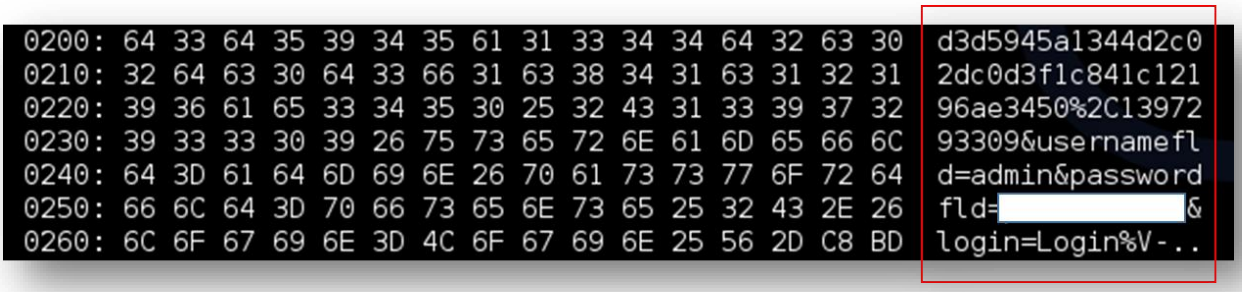
เป็นเหตุให้ข้อมูลความลับ ไม่ว่าจะเป็น key ที่ใช้ถอดรหัสข้อมูล รวมถึงข้อมูลอื่น ๆ เช่น username/password ถูกเข้าถึงได้โดย Hacker (ขอแถมอีกนิดว่าการที่ช่องโหว่นี้ได้ชื่อว่า Heartbleed เนื่องจากตัว Extension ตัวหนึ่งใน OpenSSL Library ชื่อว่า “Heartbeat” เป็นตัวการให้เกิดการรั่วไหลของข้อมูล)

## Heartbleed Bug ได้ข้อมูลหมดทุกอย่างใน RAM เลยหรือ?

คำตอบคือ ไม่ จะได้ข้อมูลเฉพาะของ Application ที่ใช้งาน OpenSSL Library นั้น ๆ เช่น สมมติว่า มีเครื่อง server 1 เครื่อง ให้บริการ HTTPS Web, VPN, Email แล้วทั้ง 3 บริการนี้มีช่องโหว่ Heartbleed Bug เหมือนกันหมด การโจมทีไปที่ VPN จะไม่ได้ข้อมูลใน RAM ของ Web และ Email ได้เฉพาะ VPN เองเท่านั้น (หากสงสัยว่าทำไม ต้องตอบว่านี่คือการทำงานปกติของระบบคอมพิวเตอร์ โปรแกรมต่าง ๆ ที่ทำงานอยู่ใน RAM จะรู้สึกเหมือนกับว่าตัวมันเองใช้งาน RAM อยู่เพียงผู้เดียว ทั้ง ๆ ที่จริงแล้วมีโปรแกรมนับร้อยทำงานอยู่)




รูปที่ 1: ตัวอย่างการรั่วไหลของข้อมูลจาก RAM จากช่องโหว่ Heartbleed




รูปที่ 2: ตัวอย่างข้อมูลสำคัญที่ได้

## ช่องโหว่นี้เกิดกับ OpenSSL version ใดบ้าง?

OpenSSL version 1.0.1a – 1.0.1f

OpenSSL version 1.0.1:beta1 – 1.0.1:beta3

OpenSSL version 1.0.2-beta1

## อยากทดสอบว่าโดเมนของท่านจะโดนโจมตีได้หรือไม่?

สามารถใช้บริการได้ที่ **http://www.tisa.or.th/heartbleed**

โดยระบุโดเมนที่ต้องการตรวจสอบในช่องใส่โดเมนจากนั้นคลิกที่ปุ่ม GO

## ในส่วนของผู้ดูแลระบบจะรับมือช่องโหว่ได้อย่างไร?

1. ทำการปิดช่องโหว่ ซึ่งทำได้โดย

1.1 ทำการอัพเดท software OpenSSL และตรวจสอบหมายเลข version ให้แน่ชัด ว่า version ของ software ได้รับการอัพเดทแล้ว

1.2 หากต้องการใช้ version เดิม ให้ทำการ recompile OpenSSL Library ใหม่แล้วจึงนำมาใช้งาน (ข้อมูลเพิ่มเติมได้ที่ heartbleed.com) เนื่องจาก OpenSSL เป็น Open Source Software

1.3 ผู้ดูแลระบบสามารถดูรายชื่อ product ที่ได้รับผลกระทบจากช่องโหว่ และอาจอยู่ในความดูแลของท่านได้ที่

http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=720951&SearchOrder=4

2. หากตรวจสอบแล้วพบว่ามีช่องโหว่จริง ควรประกาศให้ผู้ใช้งานได้รับทราบ เพราะเราไม่สามารถรู้ได้ว่าก่อนหน้าที่เราจะรู้ตัวเราถูกโจมตีหรือไม่ (เป็นอีกหนึ่งความพิเศษของช่องโหว่นี้) และเสียหายไปเท่าไร เพื่อให้ผู้ใช้งานได้รับมือกับการรั่วไหลของข้อมูลได้อย่างทันท่วงที

3. สร้าง X.509 Certificates ใหม่ เพราะเป็นไปได้ว่าถ้าหากถูกโจมตี ข้อมูลของ Certificates อาจรั่วไหลไปได้เช่นกัน ถ้าหากยังใช้ Certificate เดิมที่ข้อมูลรั่วไหลไปแล้ว ต่อให้เราปิดช่องโหว่ที่ OpenSSL แต่ข้อมูลใน Certificate เดิมก็สามารถนำมาใช้ถอดรหัสข้อมูลใหม่ ๆ ได้

## ผู้ใช้งานหากได้รับประกาศช่องโหว่จากผู้ให้บริการควรทำอย่างไร?

รีบเปลี่ยนรหัสผ่านและข้อมูลสำคัญที่ใช้ยืนยันตัวตนกับผู้ให้บริการทันที เพราะเราไม่สามารถแน่ใจได้ว่าข้อมูลของเราเองอยู่ใน RAM ขณะที่เกิดการโจมตีหรือไม่ หากการโจมตีเคยเกิดขึ้นจริง

## หน่วยงานในประเทศไทยที่สามารถขอความช่วยเหลือได้

**ThaiCERT**

Email : report@thaicert.or.th

Hotline: 1212

**Reference: http://heartbleed.com**