



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 การโจมตีไปที่ VPN จะไม่ได้ข้อมูลใน RAM ของ Web และ Email ได้เฉพาะ VPN เองเท่านั้น (หากสงสัยว่าทำไม ต้องตอบว่านี่คือการทำงานของระบบคอมพิวเตอร์ โปรแกรมต่าง ๆ ที่ทำงานอยู่ใน RAM จะรู้สึกเหมือนกับว่าตัวมันเองใช้งาน RAM อยู่เพียงผู้เดียว ทั้ง ๆ ที่จริงแล้วมีโปรแกรมนับร้อยทำงานอยู่)

```
[+]Successfully Exploited OpenSSL Heartbeat Extension:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 +..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f....."
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ...E.D..../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 4C 61 6E 67 ...#.Lang
00e0: 75 61 67 65 3A 20 65 6E 2D 55 53 2C 65 6E 3B 71 uage: en-US,en;q
00f0: 3D 30 2E 35 0D 0A 41 63 63 65 70 74 2D 45 6E 63 =0.5..Accept-Enc
0100: 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 oding: gzip, def
0110: 6C 61 74 65 0D 0A 52 65 66 65 72 65 72 3A 20 68 late..Referer: h
0120: 74 74 70 73 3A 2F 2F 32 30 32 2E 32 38 2E 33 37 ttps://
0130: 2E 32 35 33 2F 0D 0A 43 6F 6F 6B 69 65 3A 20 63 .253/..Cookie: c
0140: 6F 6F 6B 69 65 5F 74 65 73 74 3D 31 33 39 37 32 ookie test=13972
0150: 39 36 39 30 39 3B 20 50 48 50 53 45 53 53 49 44 96909; PHPSESSID
0160: 3D 61 65 31 38 37 33 38 35 65 35 34 37 39 37 66 =ae187385e54797f
0170: 33 65 35 65 30 37 34 31 62 39 37 32 34 34 39 33 3e5e0741b9724493
0180: 32 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 2..Connection: k
0190: 65 65 70 2D 61 6C 69 76 65 0D 0A 0D 0A E4 05 7C eep-alive.....|
01a0: CC C5 D9 8C 48 F9 DB 35 6B FB 77 A0 00 6E 0F 79 ...H..5k.w.n.y
01b0: BC 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E 0E .....
01c0: 6F 52 58 B7 9E E9 3D 0B A0 11 48 F2 55 D3 82 F8 oRX...=...H.U...
01d0: EE 50 97 11 B0 CA 8D 5D 19 E7 27 EC 8D 44 25 65 .P.....]...'..D%e
01e0: AA 1C 54 C6 76 20 31 32 36 0D 0A 0D 0A 5F 5F 63 ..T.v 126...._c
01f0: 73 72 66 5F 6D 61 67 69 63 3D 73 69 64 25 33 41 srf_magic=sid%3A
0200: 64 33 64 35 39 34 35 61 31 33 34 34 64 32 63 30 d3d5945a1344d2c0
0210: 32 64 63 30 64 33 66 31 63 38 34 31 63 31 32 31 2dc0d3f1c841c121
```

รูปที่ 1: ตัวอย่างการรั่วไหลของข้อมูลจาก RAM จากช่องโหว่ Heartbleed

```
0200: 64 33 64 35 39 34 35 61 31 33 34 34 64 32 63 30 d3d5945a1344d2c0
0210: 32 64 63 30 64 33 66 31 63 38 34 31 63 31 32 31 2dc0d3f1c841c121
0220: 39 36 61 65 33 34 35 30 25 32 43 31 33 39 37 32 96ae3450%2C13972
0230: 39 33 33 30 39 26 75 73 65 72 6E 61 6D 65 66 6C 93309&usernamefl
0240: 64 3D 61 64 6D 69 6E 26 70 61 73 73 77 6F 72 64 d=admin&password
0250: 66 6C 64 3D 70 66 73 65 6E 73 65 25 32 43 2E 26 fld= &
0260: 6C 6F 67 69 6E 3D 4C 6F 67 69 6E 25 56 2D C8 BD login=Login%V-..
```

รูปที่ 2: ตัวอย่างข้อมูลสำคัญที่ได้

## ช่องโหว่นี้เกิดกับ OpenSSL version ไตบ้าง?

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 ทำการอัปเดต software OpenSSL และตรวจสอบหมายเลข version ให้แน่ชัด ว่า version ของ software ได้รับการอัปเดตแล้ว

1.2 หากต้องการใช้ version เดิม ให้ทำการ recompile OpenSSL Library ใหม่แล้วจึงนำมาใช้งาน (ข้อมูลเพิ่มเติมได้ที่ [heartbleed.com](http://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. หากตรวจสอบแล้วพบว่ามิช้องโหว่จริง ควรประกาศให้ผู้ใช้งานได้รับทราบ เพราะเราไม่สามารถรู้ได้วก่อนหน้าที่เราจะรู้ตัวเราถูกโจมตีหรือไม่ (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](mailto:report@thaicert.or.th)

Hotline: 1212

Reference: <http://heartbleed.com>