Heartbleed beats hard

Geschichten aus 1000 und einem Netzwerk

Curesec GmbH

- Technische IT-Security
- Security Audits
- Tiger Team Audits
- Mobile Phone Untersuchung (Android/iOS)
- Produktbegleitung
- Trainings

Curesec GmbH

- Tools:
  - Sicherheitsuntersuchungen
  - hbad – Untersuchung von Clients
- Schwachstellen wie z.B. in:
  - WhatsApp
  - Android
- Guidelines z.B.:
  - Banking Security

Curesec GmbH

- Sitz ist in Berlin
- Team besteht aus 7 Mitarbeitern
- Arbeit findet International statt
- Flyer liegen aus

Eckdaten

- Veröffentlicht am 7. April 2014
- Gefunden von zwei Firmen
  - Codenomicon und Google
- Bug existiert seit Dezember 2011
- Betrifft alle aktuellen Versionen 1.0.1 [abcdef]
- Patch 1.0.1g oder alte Version 0.9.8

Was passiert?

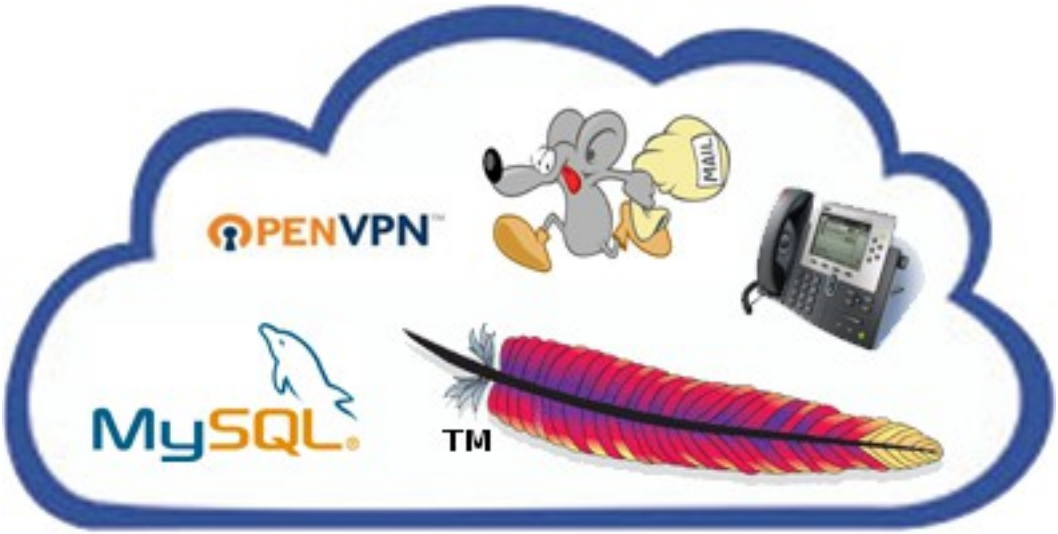
- Heartbeat -> Erweiterung
- Sollte die Sitzung aufrecht erhalten
- Speicherdaten werden vom Server UND Client versendet
- Daten aus dem Prozessspeicherinhalt

Wer ist anfällig?

Jeder, der Software benutzt, die mit den problematischen OpenSSL-Versionen gelinkt sind UND die Extension eingeschaltet ist!

Was ist anfällig?

- Serverseitig:
  - Webserver
  - Datenbankserver
  - Emailserver
  - VoIP-Systeme
  - VPN
  - Custom software
  - mit OpenSSL gelinkte Software



Webserver Beispiel

```
000000C8  1C AB 1F 04  04 04 04 04  29 0D 0A 43  6F 6F 6B 69  65 3A 20 44  ........)..Cookie: D
000000DC  53 4C 61 73  74 41 63 63  65 73 73 3D  31 33 39 39  58 58 58 58  SLastAccess=1399XXXX
000000F0  58 58 3B 20  44 53 46 69  72 73 74 41  63 63 65 73  73 3D 31 33  XX; DSFirstAccess=13
00000104  39 39 33 58  58 58 58 58  3B 20 44 53  49 44 3D 33  34 35 65 63  993XXXXX; DSID=345ec
00000118  36 34 33 66  33 34 35 58  58 58 58 58  58 58 58 58  58 58 58 58  643f345XXXXXXXXXXXXX
0000012C  58 58 58 58  58 58 58 3B  20 70 61 74  68 3D 2F 3B  20 73 65 63  XXXXXXX; path=/; sec
00000140  75 72 65 3B  20 58 58 58  58 58 58 58  58 58 58 58  58 58 58 58  ure; XXXXXXXXXXXXXXX
00000154  58 58 3D 58  58 58 58 58  58 58 58 58  73 72 76 2E  58 58 58 58  XX=XXXXXXXXsrv.XXXX
00000168  58 58 58 2E  6C 6F 63 61  6C 2B 0D 0A  0D 0A CC 13  4A A6 7B 86  XXX.local+......J.{.
0000017C  E6 F1 49 E1  2E A0 EA BC  F9 77 B5 59  0E C8 05 05  05 05 05 05  ..I......w.Y........
00000190  E8 AF ED 0C  0C 0C 0C 0C  0C 0C 0C 0C  0C 0C 0C 0C  76 65 3C 2F  ................ve</
000001A4  77 73 61 3A  41 63 74 69  6F 6E 3E 3C  77 73 61 3A  4D 65 73 73  wsa:Action><wsa:Mess
000001B8  61 67 65 49  44 3E 75 72  6E 3A 75 75  69 64 3A 58  58 58 58 58  ageID>urn:uuid:XXXXX
000001CC  58 58 58 58  58 58 58 58  58 58 58 58  58 58 58 58  58 58 58 58  XXXXXXXXXXXXXXXXXXXX
000001E0  58 58 58 58  58 58 58 58  58 58 58 3C  2F 77 73 61  3A 4D 65 73  XXXXXXXXXXX</wsa:Mes
000001F4  73 61 67 65  49 44 3E 3C  2F 73 6F 61  70 3A 48 65  61 64 65 72  sageID></soap:Header
00000208  3E 3C 73 6F  61 70 3A 42  6F 64 79 3E  3C 77 73 64  3A 52 65 73  ><soap:Body><wsd:Res
0000021C  6F 6C 76 65  3E 3C 77 73  61 3A 45 6E  64 70 6F 69  6E 74 52 65  olve><wsa:EndpointRe
00000230  66 65 72 65  6E 63 65 3E  3C 77 73 61  3A 41 64 64  72 65 73 73  ference><wsa:Address
00000244  3E 75 72 6E  3A 75 75 69  64 3A 58 58  58 58 58 58  58 58 58 58  >urn:uuid:XXXXXXXXXX
00000258  58 58 58 58  58 58 58 58  58 58 58 58  58 58 58 58  58 58 58 58  XXXXXXXXXXXXXXXXXXXX
0000026C  58 58 58 58  58 58 3C 2F  77 73 61 3A  41 64 64 72  65 73 73 3E  XXXXXX</wsa:Address>
00000280  3C 2F 77 73  61 3A 45 6E  64 70 6F 69  6E 74 52 65  66 65 72 65  </wsa:EndpointRefere
00000294  6E 63 65 3E  3C 2F 77 73  64 3A 52 65  73 6F 6C 76  65 3E 3C 2F  nce></wsd:Resolve></
000002A8  73 6F 61 70  3A 42 6F 64  79 3E 3C 2F  73 6F 61 70  3A 45 6E 76  soap:Body></soap:Env
```

Was ist anfällig?

- Clientseitig:
  - Browser
  - Email clients
  - VoIP clients
  - VPN clients
  - Chat clients
  - Mit OpenSSL gelinkte Inhalte

Client Side Analysis

- Heartbleed Client Side Analysis Daemon
  - Tool um Software zu testen
  - Am 5. Mai veröffentlicht
  - URL: http://www.curesec.com/en/publications/tools.html

w3m Beispiel

```
0000c150  00 00 00 00 00 00 00 00  00 00 00 00 00 76 61 6c  |.............val|
0000c160  69 64 20 63 65 72 74 69  66 69 63 61 74 65 0a 20  |id certificate. |
0000c170  73 75 62 6a 65 63 74 3d  61 63 63 6f 75 6e 74 73  |subject=accounts|
0000c180  2e 67 6f 6f 67 6c 65 2e  63 6f 6d 3a 20 69 73 73  |.google.com: iss|
0000c190  75 65 72 3d 47 6f 6f 67  6c 65 20 49 6e 74 65 72  |uer=Google Inter|
0000c1a0  6e 65 74 20 41 75 74 68  6f 72 69 74 79 20 47 32  |net Authority G2|
0000c1b0  0a 0a 43 65 72 74 69 66  69 63 61 74 65 3a 0a 20  |..Certificate:. |
0000c1c0  20 20 20 44 61 74 61 3a  0a 20 20 20 20 20 20 20  |   Data:.       |
0000c1d0  20 56 65 72 73 69 6f 6e  3a 20 33 20 28 30 78 32  | Version: 3 (0x2|
0000c1e0  29 0a 20 20 20 20 20 20  20 20 53 65 72 69 61 6c  |).        Serial|
0000c1f0  20 4e 75 6d 62 65 72 3a  20 38 37 30 33 34 30 32  | Number: 8703402|
0000c200  39 32 36 34 39 34 37 35  31 36 38 32 20 28 30 78  |926494751682 (0x|
0000c210  37 38 63 38 62 32 64 39  35 61 64 30 39 62 63 32  |78c8b2d95ad09bc2|
0000c220  29 0a 20 20 20 20 53 69  67 6e 61 74 75 72 65 20  |).    Signature |
0000c230  41 6c 67 6f 72 69 74 68  6d 3a 20 73 68 61 31 57  |Algorithm: sha1W|
0000c240  69 74 68 52 53 41 45 6e  63 72 79 70 74 69 6f 6e  |ithRSAEncryption|
0000c250  0a 20 20 20 20 20 20 20  20 49 73 73 75 65 72 3a  |.        Issuer:|
0000c260  20 43 3d 55 53 2c 20 4f  3d 47 6f 6f 67 6c 65 20  | C=US, O=Google |
0000c270  49 6e 63 2c 20 43 4e 3d  47 6f 6f 67 6c 65 20 49  |Inc, CN=Google I|
0000c280  6e 74 65 72 6e 65 74 20  41 75 74 68 6f 72 69 74  |nternet Authorit|
0000c290  79 20 47 32 0a 20 20 20  20 20 20 20 20 20 56 61 6c  |y G2.        Val|
0000c2a0  69 64 69 74 79 0a 20 20  20 20 20 20 20 20 20 20  |idity.          |
0000c2b0  20 20 4e 6f 74 20 42 65  66 6f 72 65 3a 20 41 70  |  Not Before: Ap|
0000c2c0  72 20 20 39 20 31 32 3a  30 32 3a 32 37 20 32 30  |r  9 12:02:27 20|
```

Interessante Daten?

- Private Schlüssel (Zertifikate)
- Usernamen und Passwörter
- Sitzungsschlüssel (z.B. Cookies, SessionIDs)
- Video- und Voice-Kommunikation
- VPN keys
- Emails
- Formulare, z.B. Bankdaten, Kreditkartendaten

Szenario I

- Client zu Server
  - Server sendet nur Heartbeat
  - Client sammelt die privaten Daten ein und analysiert diese
- Betroffen:
  - Server im Internet und internen Netzen

Szenario II

- Client ist anfällig und verbindet sich zum Server, der Heartbeat anfragt.
  - Client sendet bereitwillig den Inhalt des Prozessspeichers zum Server
- Betroffen:
  - Alle Clients mit der anfälligen Software
  - Privatpersonen, Unternehmen, Behörden

Szenario III

- Client und Server tauschen bereitwillig ihren Prozessspeicher aus
- So haben beide etwas davon
- Betroffen:
  - Alle

Szenario IV

- Man in the middle Attack
- Umleiten von anfälligen Clients auf einen Daemon, der die Daten einsammelt
- SSL Man in the middle – direkt alles mitlesen

Ist doch aber verschlüsselt?

- Beim Sitzungsaufbau unverschlüsseltes Senden des ersten Heartbeats
  - Danach werden die Daten verschlüsselt ausgetauscht
  - Demnach reicht schon das Mitlesen der Daten an einem Router von z.B. einem großen Netzwerk
  - Ist nicht unsichtbar!

Herzblut 0x01

- Ein Unternehmen ist bereits seit Verföffentlichung der Schwachstelle mit der Reperatur beschäftigt.
- Man ist sicher, alles erledigt zu haben und wendet sich anderen Themen zu.
- Wir finden die Schwachstelle auf einem der Hauptsysteme (ca. 100.000 Kunden)

Herzblut 0x01

- Welche Daten lagen offen:
  - Login-Daten (Username/Passwörter)
  - HTTP-Daten
- Wie kam es dazu?
  - Server fuhr Dienst nicht herunter und erneut hoch
  - Stop/Start/Restart

Herzblut 0x01

- Obwohl getestet worden war, gaben “Testseiten” im Internet falsche Ergebnisse zurück.
- Angreifbarer Zeitraum nach Bekannwerden des Bugs:

4 Tage

Herzblut 0x02

- Die Schwachstelle ist dem Unternehmen bekannt, der Administrator prüft die kritischen Systeme.
- Es werden auf verschiedenen Systemen Tests durchgeführt und Patches eingespielt.
- Bei einer Untersuchung unsererseits fiel auf, dass ein System, das nicht anfällig sein sollte, angreifbar war.

Herzblut 0x02

- Das System wurde vom Admin auf einen aktuellen Stand gebracht – nur leider war der Patch vom 4. April. (Remember: 7.April)
- Es stellte sich heraus, dass damit die Schwachstelle eingebaut worden war.
- Vorher lieft auf den Systemen OpenSSL in Version 0.9.8

Herzblut 0x02

- Update kam am 4. April, wurde eingespielt am 8.April, Fix der Firewall/VPN am 11.April
- Betroffen: VPN-Zugang
- Angreifbarer Zeitraum nach einspielen des Bugs:

4 Tage

Herzblut 0x03

- Updates und Prüfung der kritischen Systeme liefen super.
- Die Zeit wurde genutzt, um sich Systeme näher anzusehen und weitere Härtungen vorzunehmen.
- Dabei wurden andere Schwachstellen gefunden.
- Angreifbarer Zeitraum:

1 Tag

Als Unternehmen?

- OpenSSL-Version 1.0.1
- Prüfen Sie alle Ihre Services
- Haben Sie kein internes Team? Wir bieten den Heartbleed Checkup an:

security@curesec.com

Vielen Dank

Marco Lux

CEO Curesec GmbH

ping@curesec.com