Whitepaper: Heartbleed

SBA Research gGmbH

Version 0.2

presse@sba-research.org

9-10. April 2014

1. Executive Summary

Eine aktuelle, relativ einfach ausnutzbare Schwachstelle, die allgemein als **"Heartbleed Bug"** bezeichnet wird, erlaubt das Auslesen potentiell hoch sensibler Informationen, die sonst nur verschlüsselt oder gar nicht übertragen werden würden. Darunter fallen je nach Anwendungsfall und Applikation verschiedene Daten. Bei HTTPS-Webanwendungen beispielsweise können dadurch private oder sensible Daten von Benutzerinnen und Benutzern ausgelesen werden.

Neben dem Zugriff auf sensible Daten kann ein Angreifender auch Sitzungsinformationen von angemeldeten Benutzerinnen und Benutzern oder private Schlüssel des Servers erbeuten. Mit diesen Daten kann ein Angreifender sich als die jeweilige Benutzerin/ der jeweilige Benutzer an der Webanwendung anmelden, verschlüsselte Kommunikation mit dem Server mitlesen bzw. nachträglich entschlüsseln.

Andere auslesbare Daten hängen dabei von dem jeweiligen Anwendungsgebiet der Webanwendung ab bzw. sind dabei von Anwendungsfall zu Anwendungsfall verschieden. Bei einer Webanwendung, die beispielsweise Kreditkartendaten verarbeitet, können diese möglicherweise von Angreifenden ausgelesen werden.

Da sich die betreffende Schwachstelle in einem elementaren Baustein für Verschlüsselungssysteme befindet, sind neben HTTPS-Webanwendungen auch andere Applikationen, die auf derselben Verschlüsselungssoftware aufbauen, potenziell betroffen:

- ✓ E-Mail-Server
- ✓ Chat-Server
- ✓ Datenbank-Server
- ✓ VPN-Systeme
- ✓ Firewalls / Gateways
- ✓ Router

Dies ist eine der gravierendsten Schwachstellen im Internet der letzten Jahre. Das konkrete Ausmaß kann bis jetzt nur erahnt werden. Die Angriffe sind dabei für AdministratorInnen und Webseitenbetreiber nicht direkt erkennbar, da diese in keinen Logfiles aufscheinen. Die Gegenmaßnahmen beinhalten die sofortige Aktualisierung von OpenSSL auf 1.0.1g sowie die Erneuerung der SSL-Zertifikate.

Da nicht feststellbar ist, ob und inwieweit Speicher ausgelesen wurde, sollten alle bestehenden Sessions und Cookies ungültig gemacht, die Zugangsdaten für alle Anwender erneuert und neue Schlüsselpaare und Zertifikate generiert werden.

Die identifizierte Schwachstelle existiert seit rund zwei Jahren, erst die kommenden Monate werden zeigen, ob diverse Personen oder Institutionen bereits früher von dieser Lücke wussten und diese möglicherweise in den letzten Monaten ausgenutzt haben.

SBA Research hat am 9. April 2014 auf Grund der akuten Bedrohungslage einen Scan aller österreichischen IP-Adressen (ca. 12 Millionen) durchgeführt.

Dabei wurden 121.420 IP-Adressen identifiziert, die auf eine HTTPS-Anfrage bei Webseiten antworteten. Jeder dieser Server kann eine oder eine Vielzahl von Webseiten beheimaten. Von diesen knapp 120.000 Systemen sind nach aktueller Erkenntnis (10. April, 11:00) **circa noch 6% oder in absoluten Zahlen 7.014 Systeme potentiell verwundbar**. Dieser Scan wird im Laufe der nächsten Tage regelmäßig wiederholt, um die aktuelle Sicherheitslage fortlaufend zu dokumentieren. Im Gegensatz zur Analyse von cert.at, welche Domains mit der Endung ".at"

überprüft hat, bezieht sich diese Analyse auf österreichische IP-Adressen[1]. Eine Diskrepanz der ermittelten Werte ergibt sich daraus, dass ".at" Domains nicht notwendigerweise auf österreichischen Servern gehostet sein müssen. Andererseits können mehrere Domains unter einer einzigen IP-Adresse erreichbar sein.

Eine kostenlose Bedrohungsanalyse Ihrer externen IP-Range können Sie unter **heartbleed@sba-research.at** anfordern.

Inhalt

1. Executive Summary 1

2. Auslesbare Informationen & Auswirkungen 4

3. Die Heartbleed-Schwachstelle 5

4. Aktuelle Situation in Österreich (09.04.2014) 6

5. Gegenmaßnahmen und Serviceüberprüfung 6

Schritt 0: Bin ich betroffen? 6

Schritt 1: Update der Software 8

Schritt 2: Erneuern aller Schlüssel / Zertifikate 8

Perfect Forward Secrecy 9

Schritt 3: Neustarten aller betroffenen Services 9

6. Technische Details zu Heartbleed 9

7. Wie sollten Benutzerinnen und Benutzer aktuell reagieren? 11

8. Weiterführende Informationen 12

[1] Quelle: http://ripe.net

2. Auslesbare Informationen & Auswirkungen

Das Auslesen des Hauptspeichers des betroffenen Server-Prozesses erlaubt es, eine Vielzahl an verschiedenen Informationen aus dem System zu extrahieren, z.B.:

- ✓ Session-Information
- ✓ Credentials/Zugangsdaten/Usernamen/Passwörter
- ✓ SSL Private Keys
- ✓ Cookies
- ✓ E-Mails
- ✓ sonstige vertrauliche Daten, wie z.B. Kreditkartendaten auf Webseiten, die Kreditkarten verarbeiten.

Im Prinzip sind sämtliche Daten, die unverschlüsselt zum Zeitpunkt der Attacke im Hauptspeicher des betreffenden Prozesses liegen, potentiell kompromittiert.

Stellen Sie sich vor, Sie haben gestern bei einem Webshop, der die Schwachstelle noch nicht behoben hatte, einen Artikel bestellt und Ihre Kreditkartendaten eingegeben:

Was kann Ihnen realistisch passieren?

a) Ihre Kreditkartendaten wurden gestohlen, also müssten Sie diese proaktiv sperren lassen.

b) Das Passwort wurde gestohlen, Sie sollten dieses ändern, hoffentlich verwenden Sie die gleiche Kombination aus E-Mail-Adresse und Passwort auf keiner anderen Webseite, sonst sind diese auch kompromittiert.

c) Ihre persönlichen Daten, also Adresse, Telefonnummer usw. wurden abgesaugt.

Was kann dem Betreiber zusätzlich passieren?

d) Es wurden **Administrationspasswörter** kompromittiert.

e) Es wurden das **Zertifikat** und der **Private Key**, die zum Verschlüsseln der Verbindung verwendet werden, gestohlen, mit diesen kann nun sämtlicher verschlüsselter Netzwerkverkehr aufgebrochen werden.

Stellen Sie sich vor, sie haben gestern ein sensibles E-Mail über einen Webmail-Server, der die Schwachstelle noch nicht behoben hatte, versendet:

Was kann Ihnen realistisch passieren?

a) Ihr E-Mail wurde gestohlen und könnte jederzeit veröffentlich werden. Erwägen Sie, als größeres Unternehmen eine Krisenkommunikationsstrategie vorzubereiten. Wenn Sie z.B. Vorstand einer AG sind, könnte dies während einer sensiblen Merger-Phase zu sehr weitreichenden Folgen führen.

b) Ihr Passwort wurde gestohlen, Sie sollten dieses ändern, falls Sie die gleiche Kombination aus E-Mail-Adresse und Passwort auf anderen Webseiten verwenden, sind diese auch kompromittiert.

c) Alle Ihre E-Mails wurden mit dem gewonnen Passwort heruntergeladen oder jemand schreibt E-Mails/Nachrichten/Content nun in Ihrem Namen.

Was kann dem Betreiber zusätzlich passieren?

d) Es wurden **Administrationspasswörter** kompromittiert, d.h. alle E-Mails des Servers sind in Gefahr.

e) Es wurden das **Zertifikat** und der **Private Key** gestohlen, mit diesen kann nun sämtlicher verschlüsselter Netzwerkverkehr aufgebrochen werden.

3. Die Heartbleed-Schwachstelle

Heartbleed beschreibt eine Sicherheitslücke, die in der populären OpenSSL-Bibliothek gefunden wurde. OpenSSL kommt in einer Vielzahl von Software zum Einsatz um Verbindungen zu verschlüsseln. Die momentan populärsten Webserver, **Apache** und **nginx**, verwenden zum Beispiel OpenSSL für HTTPS-Verbindungen. Diese frei verfügbare Software kommt neben dem Linux-Umfeld oft auch im Windows-Umfeld als sog. **Proxy** zum Beispiel bei Windows IIS (Internet Information Server) zum Einsatz. Obwohl IIS als solche nicht durch Heartbleed verwundbar sind, kann der Einsatz von Proxy-Software zu verwundbaren Webservices führen. Neben Webservices ist generell jegliche Software betroffen, die OpenSSL verwendet, wie beispielsweise E-Mailserver oder bestimme VPN-Server. Heartbleed nützt einen Programmierfehler in der Heartbeat-Erweiterung von OpenSSL aus und ermöglicht Angreifenden das Auslesen von Speicherbereichen von Servern. Diese Speicherbereiche beinhalten oft sensible Nutzerdaten wie Passwörter oder Session-Informationen. Im schlimmsten Fall können Angreifende sogar die privaten Schlüssel von geschützten Verbindungen auslesen. Bei Servern ohne Perfect Forward Secrecy (TLS 1.2) können Angreifende,

welche den Netzwerkverkehr aufgezeichnet haben, im Nachhinein den Kommunikationsinhalt entschlüsseln.

4. Aktuelle Situation in Österreich (09.04.2014)

SBA Research hat am 09.04.2014 auf Grund der akuten Bedrohungslage einen Scan aller österreichischen IP-Adressen (ca. 12 Millionen) durchgeführt. Dabei wurden 121.420 IP-Adressen identifiziert, die auf eine HTTPS-Anfrage bei Webseiten antworten. Jeder dieser Server kann hierbei eine oder eine Vielzahl von Webseiten beheimaten.

Von diesen knapp 120.000 Systemen sind nach aktueller Erkenntnis circa noch 6% oder in absoluten Zahlen 7.014 Systeme potentiell verwundbar.

5. Gegenmaßnahmen und Serviceüberprüfung

Die folgende Beschreibung des Updatevorgangs bezieht sich in erster Linie auf Debian/Ubuntu Server. Jedoch sollten die einzelnen Schritte auf anderen Linux-Distribution unter Zuhilfenahme der entsprechenden Paket-Manager ebenfalls reproduzierbar sein.

Schritt 0: Bin ich betroffen?

Laut aktuellem Kenntnisstand sind folgende Versionen anfällig:

- ✓ OpenSSL 1.0.1 bis 1.0.1f (inklusive)

Folgende Versionen sind laut aktuellem Kenntnisstand **nicht** anfällig:

- ✓ OpenSSL 1.0.1g
- ✓ OpenSSL 1.0.0 branch
- ✓ OpenSSL 0.9.8 branch

Um die installierte Version von openssl zu überprüfen kann folgender Befehl verwendet werden:

```
$ openssl version -a
```

Um zu überprüfen, ob die "Heartbeat"-Funktionalität für eine HTTPS-Seite aktiviert ist, kann folgendes openssl Kommando verwendet werden:

```
$ openssl s_client -connect example.com:443 -tlsextdebug 2>&1
```

Um ihren Server auf die betreffende Schwachstelle zu überprüfen gibt es mehrere Möglichkeiten. Vielfach wird hierbei auf Webseiten verwiesen (z.B. http://filippo.io/Heartbleed/ oder http://possible.lv/tools/hb/). Wir raten jedoch vom Einsatz der betreffenden Webseiten ab, um eine mögliche Verwundbarkeit eines bestimmten Servers nicht an Dritte preiszugeben. Wir empfehlen daher, die Sicherheitslücke mit folgenden Skripten zu überprüfen:

- ✓ Heartbleed (GO):

  Einfaches GO-Script um Server zu überprüfen:
  https://github.com/FiloSottile/Heartbleed
  ```
  $ Heartbleed example.com:443
  ```

- ✓ Check SSL Heartbleed (Perl):

  Das Script ermöglicht neben HTTPS eine Überprüfung von gängigen E-Mail-Services:
  https://github.com/noxxi/p5-scripts/blob/master/check-ssl-heartbleed.pl

  Für die Überprüfung von **Webservern**:
  ```
  $ ./check-ssl-heartbleed.pl example.com:https
  ```

  Für die Überprüfung von **E-Mail-Services**:
  ```
  $ ./check-ssl-heartbleed.pl example.com:imaps
  ```

- ✓ Inzwischen unterstützen gängige Sicherheitstools die Überprüfung der Sicherheitslücke:
  - **Metasploit**: http://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_heartbleed
  - **Nmap**: http://nmap.org/nsedoc/scripts/ssl-heartbleed.html
  - **OpenVAS**: https://gist.github.com/RealRancor/10140249
  - **Nessus**: http://www.tenable.com/plugins/index.php?view=single&id=73412

- ✓ Weiters existieren bereits Regeln für Intrusion Detection Tools, um den Angriff im Netzwerk zu erkennen:
  - **Snort**:
    - http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/
    - http://vrt-blog.snort.org/2014/04/heartbleed-memory-disclosure-upgrade.html
  - **Bro**:
    - http://blog.bro.org/2014/04/detecting-heartbleed-bug-using-bro.html

Schritt 1: Update der Software

Die Beschreibungen des Updatevorgangs beziehen sich in erster Linie auf Debian/Ubuntu Server. Jedoch sollten die einzelnen Schritte auf anderen Linux-Distribution unter Zuhilfenahme der entsprechenden Packet-Manager ebenfalls reproduzierbar sein.

Das betroffene System kann über den Packet-Manager aktualisiert werden:

```
$ apt-get update
$ apt-get install openssl libssl
```

Nachdem die entsprechenden Updates durchgeführt wurden, sollte die Ausgabe von "`openssl version`" ein Erstelldatum nach dem 7.4.2014 aufweisen. Da Debian/Ubuntu die Änderungen in eine früher Version portiert hat, ist die Versionsnummer eventuell nach wie vor kleiner 1.0.1g.

```
$ openssl version -a
[...]
built on: Mon Apr  7 20:33:29 UTC 2014
[...]
```

Schritt 2: Erneuern aller Schlüssel / Zertifikate

Da davon ausgegangen werden muss, dass die Schwachstelle bereits erfolgreich ausgenutzt wurde, wird dringend empfohlen, alle Schlüssel und Zertifikate, die mit SSL verwendet werden bzw. von Programmen verwendet werden, die libssl importieren, zu erneuern.

Perfect Forward Secrecy

Sollten im Zuge dieser Schwachstelle private Schlüssel kompromittiert worden und kein **Perfect Forward Secrecy** aktiviert sein, können alle bis dorthin aufgezeichneten und über SSL verschlüsselten Verbindungen entschlüsselt werden.
In Perfect Forward Secrecy wird für jede Sitzung über Diffie Hellman ein eigener Sitzungsschlüssel ausgehandelt, was eine Entschlüsselung der Daten im Nachhinein unmöglich macht - auch, wenn der private Schlüssel gestohlen wurde.

Schritt 3: Neustarten aller betroffenen Services

Nach der Erneuerung aller Schlüssel und Zertifikate sollten die beeinflussten Prozesse neu gestartet werden. Zusätzlich sollten alle aktiven Sitzungen abgebrochen werden, um sie auf diese Art zu einem Neuaufbau zu zwingen. Mit dem folgenden Befehl kann überprüft werden, welcher Service noch die bereits entfernte Version von `libssl` verwendet:

```
$ lsof -n | grep ssl | grep DEL
```

Im letzten Schritt müssen demnach alle Services, welche `libssl` verwenden, neu gestartet werden (falls dies nicht bereits durch den Packet-Manager veranlasst wurde), bzw. der Rechner neu gestartet werden, um so alle Prozesse neu zu starten.

6. Technische Details zu Heartbleed

Der Fehler liegt in der mangelhaften Längenprüfung von Heartbeat-Nachrichten in OpenSSL, wie spezifiziert in RFC 6520[2]. Damit lassen sich bis zu 64 Kb Speicher auslesen, die nicht initialisiert sind und damit alte Inhalte des Heaps beinhalten können.

Neben Web- und E-Mail-Servern sind auch Netzwerk- und Securityprodukte von Herstellern wie Checkpoint, Cisco, F5, Juniper & Riverbed verwundbar.

Der folgende Link enthält die Sourcecode-Änderungen, um die Schwachstelle zu beheben: http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db9023b881d7cd9f379b0c154650d6c108e9a3

[2] https://tools.ietf.org/html/rfc6520

Der verwundbare Code befindet sich in der Datei ssl/d1_both.c in der Funktion dtls1_process_heartbeat(SSL *s) und wird im Folgenden analysiert. Die in grün ergänzten Kommentare erklären den Code.

```
// erhaltener Heartbeat-Request
unsigned char *p = &s->s3->rrec.data[0], *pl;
….
unsigned int payload;
unsigned int padding = 16; /* Use minimum padding */
….
// Länge der Heartbeat-Daten auslesen (durch den Angreifenden
manipulierbar!)
n2s(p, payload);
….
// "zufälliger" Speicher wird alloziert, wobei die Größe des Speichers vom
Angreifenden bestimmt werden kann (bis zu 64 Kb)
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
….
// der Server kopiert die erhaltenen Daten vom Client in den allozierten
Speicher, wobei dieser die Länge nicht eigenständig prüft, sondern den
Angaben des Clients (Angreifender) vertraut. Dies kann dazu führen, dass
der Server Speicher alloziert, der nicht vollständig durch den Server
überschrieben und diesen an den Client zurücksendet.
r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);
```

Die gepatchte Version enthält die fehlenden Längenüberprüfungen.

```
/* Read type and payload length first */
// Prüfung ob die angegebene Länge des Pakets die Mindestlänge erfüllt
if (1 + 2 + 16 > s->s3->rrec.length)
      return 0; /* silently discard */
hbtype = *p++;
n2s(p, payload);
// Prüfung ob die angegebene Länge des Pakets die tatsächliche Länge nicht
überschreitet
if (1 + 2 + payload + 16 > s->s3->rrec.length)
      return 0; /* silently discard per RFC 6520 sec. 4 */
```

7. Wie sollten Benutzerinnen und Benutzer aktuell reagieren?

Nachdem fast alle der großen Internetanbieter betroffen sind, ist **von Seiten der Benutzerinnen und Benutzer eine rasche Reaktion notwendig**. Konkret sollten ab dem Zeitpunkt, an dem der betroffene Dienst gepatcht (also sicherheitstechnisch abgesichert und aktualisiert) wurde, das Passwort von allen BenutzerInnen dieses Dienstes neu vergeben werden.

Nach derzeitigen Informationen sollten Benutzerinnen und Benutzer der folgenden meistverwendeten Dienste sofort ihr Passwort ändern:

- ✓ Facebook
- ✓ Tumblr
- ✓ Google / Gmail
- ✓ Yahoo / Yahoo Mail
- ✓ Amazon Web Services (nicht Amazon Shops!)
- ✓ Dropbox
- ✓ Lastpass
- ✓ SoundCloud
- ✓ Wunderlist

Eine aktuelle Liste der anfälligen Systeme findet sich auf
http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

8. Weiterführende Informationen

Offizielle Advisories:

- CVE 2014-0160: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- http://www.heartbleed.com

PoC Software zum Testen der Heartbleed-Schwachstelle:

- https://gist.github.com/takeshixx/10107280
- https://gist.github.com/sh1n0b1/10100394
- https://gist.github.com/mpdavis/10171593 (Suche nach Benutzersitzungen)
- http://packetstormsecurity.com/files/126069/Heartbleed-User-Session-Extraction.html (Suche nach Benutzersitzungen)

Weitere Tools:

- http://packetstormsecurity.com/files/126068/Heartbleed-Honeypot-Script.html (Honeypot)

Beschreibungen der Schwachstelle:

- Matthew Green: http://blog.cryptographyengineering.com/2014/04/attack-of-week-openssl-heartbleed.html
- Ivan Ristic: https://community.qualys.com/blogs/securitylabs/2014/04/08/ssl-labs-test-for-the-heartbleed-attack