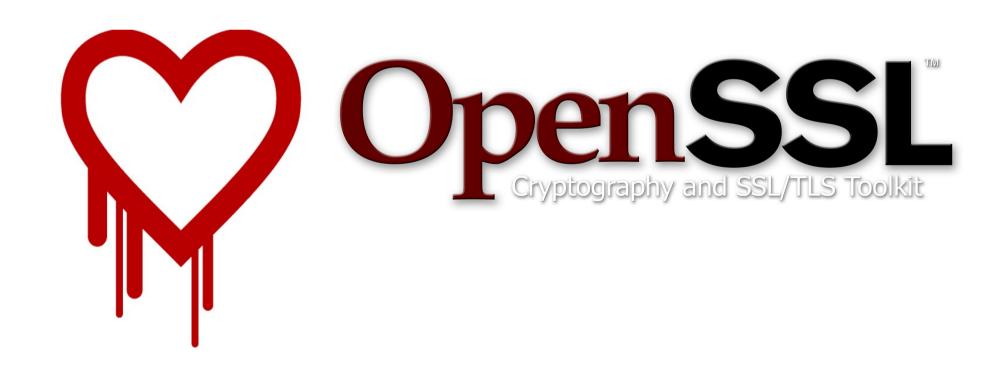
Heartburn from Heartbleed forces wideranging rethink in open source world

By Alex Hesselgrave



What is OpenSSL?

- Backbone of Internet Security
- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- OpenSSL implements both in a convenient toolkit library
- Most importantly, FREE and OPEN SOURCE

What is Heartbleed?

- Heartbeat feature of OpenSSL 1.0.1
- Length = number of bytes received
- Payload = number of bytes to send back

```
struct
  HeartbeatMessageType type;
  uint16 payload length; //Important!!!!
  opaque payload[HeartbeatMessage.payload length];
  opaque padding[padding length];
} HeartbeatMessage;
struct ssl3_record_st
  unsigned int length; /* How many bytes available */
  [\ldots]
  unsigned char *data; /* pointer to the record data */
  [\ldots]
} SSL3 RECORD;
```

Discovery of the bug

- Discovered by Google and Codenomicon in the beginning of April
- Critical testing led to the discovery of information leak
- Publicly reported by OpenSSL on April 7th

Popularization

- Www.heartbleed.com
- Codenomicon Heartbleed logo and site
- Extremely quick media coverage

The Future of Open Source

- Core Infrastructure Initiative
- Google, Facebook, Microsoft, IBM, Cisco, etc.
- OpenSSL alone is the backbone for about 500k websites
- "We use a lot of open-soure software because we hope that [...] somebody has spent the time to make sure their investment is protected."
- Need for funding and rigorous code review