OpenSSL, rather TLS woes continue!

Contributed by Michael Felt

OK, I am already weeks behind - log-jam is the name to know these days - unless your name is LibreSSL (see below).

From the CVE text (see http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000) I see
not even TLS1.2 is safe from (I guess) design errors. At the moment I am asking myself: "What is
DHE_EXPORT?". If it is an environment variable - yeah for me, I do not use any envrionment variables.
And, now I understand better why LibreSSL disabled all settings via environment variables in LibreSSL-2.2.0
(see http://ftp.openbsd.org/pub/OpenBSD/LibreSSL/libressl-2.2.0-relnotes.txt)

The juicy parts... * Fixes for the following issues are integrated into
LibreSSL 2.1.7 and 2.2.0:

- CVE-2015-1788 - Malformed ECParameters causes infinite loop
- CVE-2015-1789 - Exploitable out-of-bounds read in X509_cmp_time
- CVE-2015-1792 - CMS verify infinite loop with unknown hash function
  (this code is not enabled by default)

* The following CVEs did not apply to LibreSSL or were fixed in earlier
releases:

- CVE-2015-4000 - DHE man-in-the-middle protection (Logjam)
- CVE-2015-1790 - PKCS7 crash with missing EnvelopedContent
- CVE-2014-8176 - Invalid free in DTLS

* Fixes for the following CVEs are still in review for LibreSSL

- CVE-2015-1791 - Race condition handling NewSessionTicket

Note: This will likely be the last 2.2.x release with support for SSLv3, as it
will be removed entirely from the main LibreSSL tree.