Internet Storm Center Briefing: June 5th 2014 OpenSSL Patches

Johannes B. Ullrich, Ph.D.
## Summary

<table>
<thead>
<tr>
<th>CVE</th>
<th>Description</th>
<th>Versions</th>
<th>Client Rating</th>
<th>Server Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-0224</td>
<td>SSL/TLS MITM</td>
<td>Server: 1.0.1 Client: all</td>
<td>Critical</td>
<td>Important</td>
</tr>
<tr>
<td>2014-0221</td>
<td>DTLS recursion DoS</td>
<td>All</td>
<td>Important</td>
<td>Not Affected</td>
</tr>
<tr>
<td>2014-0195</td>
<td>DTLS invalid Fragment Code Exec.</td>
<td>All</td>
<td>Critical</td>
<td>Critical</td>
</tr>
<tr>
<td>2014-0198</td>
<td>SSL_MODE_RELEASE_BUFFERS DoS</td>
<td>1.0.0, 1.0.1</td>
<td>Important</td>
<td>Important</td>
</tr>
<tr>
<td>2010-5298</td>
<td>SSL_MODE_RELEASE_BUFFERS injection</td>
<td>1.0.0, 1.0.1</td>
<td>Important</td>
<td>Important</td>
</tr>
<tr>
<td>2014-3470</td>
<td>Anonymous ECDH DoS</td>
<td>0.9.8, 1.0.0, 1.0.1</td>
<td>Important</td>
<td>Not Affected</td>
</tr>
<tr>
<td>2014-0076</td>
<td>ECDSA Side Channel</td>
<td>1.0.0, 0.9.8 (1.0.1)</td>
<td>Less Important</td>
<td>Less Important</td>
</tr>
</tbody>
</table>
Current Version

0.9.8 za

1.0.0m

1.0.1h
Subtle SSL handshake timing bug
Affects TLS and could allow for a MitM attack (not just DTLS)
Root cause: Change Cipher Spec (CCS) message is accepted before all prerequisites have been processed
Flaw existed in OpenSSL “since the beginning”
Effect: an empty master secret is used
Who uses is Vulnerable?

- Who is not vulnerable?
  - Servers running OpenSSL = 1.0.1
  - Client AND Server have to be vulnerable
• An invalid DTLS handshake to vulnerable client can crash the client.
• Client is attacked
• DoS
Who uses DTLS

• SSL over UDP protocols use DTLS. Typically found in:
  – VPNs (OpenVPN)
  – VoIP (e.g. Cisco telepresence)
  – WebRTC
  – LDAP over SSL
  – SNMPv3
  – Most video/voice over SSL
• Buffer overflow caused by invalid DTLS fragments.
• Can lead to arbitrary code execution
• Can be used against client and server
• PoC details available
DTLS Fragments

• DTLS messages may be fragmented to avoid IP fragmentation
• Each DTLS fragment has three properties:
  – Total message length ("Length")
  – Fragment Offset ("Offset")
  – Fragment Size
The way it is supposed to work

• First Fragment received ("Length" > "Fragment Length")
• OpenSSL reserves "Length" bytes
• Then copies fragments into this buffer as they arrive

Assumption: All Fragments claim the same "Length" for the total message.
Why we got a bug?

- OpenSSL FAILS to check the “Length” fragments claim for the full message
- Just checks if Length > Fragment Size

- First Fragment:
  - Length: 2
  - Fragment Size: 1

- Second Fragment
  - Length: 1000
  - Fragment Size: 999
• Can cause DoS or injection of unauthenticated data.
• Only vulnerable if SSL_MODE_RELEASE_BUFFERS is used to save memory (32k per idle connection)
• Not used by default, but many developers enable it to save memory (e.g. openvpn, Apache 2.4.1, nginx)
• Setting has no effect for DTLS/SSL2
CVE-2014-3470

- Anonymous ECDH DoS Vulnerability
- Not a lot of details on exact nature of flaw
- Best practice: Disable anonymous cipher suites (e.g. in Apache !aNull enforces authentication)
Where should I start?

- Start with the inventory of OpenSSL systems that you used to mitigate “Heartbleed”
- Expedite patches as vendors make them available
- Review SSL configuration
- Monitor for server crashes
- Apply IDS Signatures as necessary
What Should I tell Management?

- This is not as bad as Heartbleed
- SSL is important because it protects our data and customer data in transit
- Accurate software inventory is critical
- OpenSSL is currently undergoing an intense review, which may lead to additional patches
http://isc.sans.edu
jullrich@sans.edu

DEV522: Defending Web Applications
SANSFIRE Baltimore June 21-30
SANS London July 14-21
SANS Boston July 28-Aug 2
http://i5c.us/defwebapp