**OpenSSL vs LibreSSL**

**Initial Remarks**

1. Forking: LibreSSL is a fork of OpenSSL. It was created as a response to the Heartbleed vulnerability, which was a serious security flaw found in OpenSSL in 2014. The LibreSSL project aimed to clean up the OpenSSL codebase and make it more secure and maintainable.
2. Focus on Security: LibreSSL has a stronger emphasis on security and code simplicity compared to OpenSSL. It removed a significant amount of code that was considered unnecessary, deprecated, or prone to security issues. The developers of LibreSSL made an effort to reduce the attack surface and eliminate potential vulnerabilities.
3. Codebase: As a result of forking, LibreSSL and OpenSSL have diverged in terms of codebase. LibreSSL took a more aggressive approach to remove or rewrite code, leading to significant differences in the implementation and structure of the libraries.
4. Platform Support: OpenSSL has broader platform support compared to LibreSSL. It is available on various operating systems and architectures, including Linux, Windows, macOS, and many more. LibreSSL initially focused on Unix-like operating systems and has expanded its platform support over time, but it may still have limitations compared to OpenSSL.
5. API Compatibility: OpenSSL and LibreSSL have similar API functions and provide comparable functionality. However, due to the codebase differences and removal of certain features, there may be some incompatibilities between the two libraries. Existing applications using OpenSSL may require modifications to work with LibreSSL.
6. Licensing: OpenSSL is licensed under the OpenSSL License, which is a permissive license. LibreSSL is licensed under the OpenBSD License, which is also a permissive license but contains some additional requirements specific to the OpenBSD project.

**Command Shortcuts to Run Programs**

|  |  |  |
| --- | --- | --- |
| @@ (path) | OpenSSL | LibreSSL |
| data/ssl/20220421\_163040\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-0\_all/testcases/id-0000820301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-0-ivtpos-8203-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  For OpenSSL:  // Additional check of Invalid Bit String Bits Left at line 146 of a\_bitstr.c:  !!!  if (i > 7) {          i = ASN1\_R\_INVALID\_BIT\_STRING\_BITS\_LEFT;          goto err;  }  For LibreSSL:  // Missing check of Invalid Bit String Bits Left at line 146 of a\_bitstr.c:  // A Bit String is composed of bytes, and since a byte is 8 bits, it doesn’t make sense for there to be 8 bits left since we could just say there are 0 bits left instead. | |
| data/ssl/20220421\_163040\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-0\_all/testcases/id-0000838001-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-0-ivtpos-8380-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as ivptos 8203, but for a different byte | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000442201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4422-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  For OpenSSL:  // Incorrectly accepts a UTC time string (YYMMDDHHMMSSZ) as it does not check for the validity of its contents (does not ensure that all the bytes are digits, allowing random characters to be used.  !!!      if (ctm->type == V\_ASN1\_UTCTIME) {          i = (buff1[0] - '0') \* 10 + (buff1[1] - '0');          if (i < 50)              i += 100;           /\* cf. RFC 2459 \*/          j = (buff2[0] - '0') \* 10 + (buff2[1] - '0');          if (j < 50)              j += 100;          if (i < j)              return -1;          if (i > j)              return 1;      }      i = strcmp(buff1, buff2);      if (i == 0)                 /\* wait a second then return younger :-) \*/          return -1;      else          return i;  }  For LibreSSL:  // Will first ensure that all its contents are digits before attempting to validate the certificate time. | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000442501-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4425-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000442801-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4428-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000443101-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4431-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000443401-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4434-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000443701-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4437-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000444001-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4440-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000444301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4443-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000444601-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4446-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000444701-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4447-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000444901-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4449-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000445201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4452-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000445301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4453-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000445501-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4455-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000445601-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4456-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000446001-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4460-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000446201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4462-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000446701-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4467-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000446901-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4469-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000448201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4482-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000448301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4483-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000448501-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4485-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000448601-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4486-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000448901-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4489-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449101-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4491-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4492-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449401-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4494-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449501-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4495-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449701-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4497-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000449801-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4498-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450001-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4500-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450101-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4501-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4503-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450401-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4504-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450601-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4506-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450701-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4507-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000450901-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4509-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451001-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4510-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451301-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4513-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451501-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4515-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |
| data/ssl/20220421\_190851\_openssl-1.0.2h-libressl-2.4.0-update-1\_tgt-1\_all/testcases/id-1000451201-openssl-1.0.2h-libressl-2.4.0-update-1-tgt-1-ivtpos-4512-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 4422 | |

**Additional Info: IVTPOS 8203/8380**

Input Bytes for IVTPOS 8203: Affected Byte at position 295: Is '20' instead of '00'

Input Bytes for IVTPOS 8380: Affected Byte at position 585: Is '40' instead of '00'

|  |  |
| --- | --- |
| OpenSSL | LibreSSL |
|  | MISSING CHECK IN LIBRESSL |

**Additional Info: IVTPOS 4422/…/4513**

Input Bytes for IVTPOS 4422: Affected Byte at position 171: Is '20' instead of '00'

Input Bytes for IVTPOS 8380: Affected Byte at position 585: Is '40' instead of '00'

|  |  |
| --- | --- |
| OpenSSL | LibreSSL |
| Missing Check  1903 if (ctm->type == V\_ASN1\_UTCTIME) {  (gdb) print \*ctm  $4 = {length = 13, type = 23, data = 0x5605f76068c0 "/10922143101Z", flags = 64}  (gdb) print buff1  $5 = "/10922143101Z\000\000\000\370\277\325\365\005V\000"  (gdb) n  1904 i = (buff1[0] - '0') \* 10 + (buff1[1] - '0');  (gdb) n  1905 if (i < 50)  (gdb) print i  $6 = -9 🡪 Invalid Expression |  |