**OpenSSL vs WolfSSL**

**Initial Remarks**

OpenSSL and wolfSSL (formerly known as CyaSSL) are two popular open-source cryptographic libraries, each with its own characteristics and features. Here are some key differences between them:

1. Codebase and Footprint: OpenSSL has a long history and a large codebase that supports a wide range of cryptographic algorithms, protocols, and features. This extensive functionality makes OpenSSL more suitable for complex and diverse use cases. On the other hand, wolfSSL is designed to be a lightweight library with a smaller code footprint, making it ideal for resource-constrained environments such as embedded systems or IoT devices.
2. Performance: OpenSSL is known for its high performance and efficiency, with optimizations and assembly-level implementations for various cryptographic algorithms. It has been extensively benchmarked and optimized over the years. wolfSSL also emphasizes performance and offers various optimizations, but its smaller code size and focus on embedded systems often make it faster and more efficient in resource-constrained environments.
3. Supported Platforms: OpenSSL has broad platform support and can be used on various operating systems, including Linux, Windows, macOS, and others. It also has extensive language bindings for different programming languages. wolfSSL, while still offering multi-platform support, has a stronger focus on embedded systems and real-time operating systems (RTOS). It is often used in scenarios where small size, fast execution, and low memory usage are critical.
4. Licensing: Licensing can be an important factor when choosing a cryptographic library. OpenSSL historically used the OpenSSL License, which some developers found to be ambiguous and had concerns about patent encumbrance. However, as of the OpenSSL 3.0 release, OpenSSL has transitioned to the Apache License 2.0, which is more permissive and widely adopted. wolfSSL, on the other hand, is dual-licensed, offering both a GPLv2 and a commercial license. The commercial license allows for more flexibility in terms of commercial usage and redistribution without requiring source code disclosure.
5. Industry Adoption: OpenSSL has been widely adopted across industries and is used in numerous applications, servers, and systems. Its long history and extensive community support have contributed to its popularity. wolfSSL, while not as widely adopted as OpenSSL, has gained popularity in embedded systems, IoT, and industries where small size and performance are critical.

When choosing between OpenSSL and wolfSSL, it's important to consider your specific requirements, the target platform, performance constraints, and licensing considerations. Both libraries have their strengths and are suitable for different use cases, so it's recommended to evaluate them based on your project's specific needs.

**Testcase Directories:**

1. 20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all
2. 20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all
3. 20220511\_171604\_openssl-1.0.2h-wolfssl-3.9.6-update-1-rank-1-20e24\_tgt-0\_all
4. 20220511\_184901\_openssl-1.0.2h-wolfssl-3.9.6-update-1-rank-1-20e24\_tgt-1\_all
5. 20220511\_191839\_openssl-1.0.2h-wolfssl-3.9.6-update-1-rank-2-d5ec8\_tgt-0\_all
6. 20220511\_214926\_openssl-1.0.2h-wolfssl-3.9.6-update-1-rank-2-d5ec8\_tgt-1\_all

|  |  |  |
| --- | --- | --- |
| @@ (path) | OpenSSL | WolfSSL |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000000901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  For OpenSSL:  // Takes into account declared length of the TLV asn.1 header, which is inconsistent with actual length of data, resulting in an error. Multiple Checks in place.  // Line 129 in asn1\_lib.c in function ASN1\_get\_object checks if max, which is the length it read from the TLV, is consistent with the actual length of data or not:  !!!         tag = i;          p++;          if (--max == 0)              goto err;      }  // Line 146 in asn1\_lib.c in function ASN1\_get\_object checks if omax, which is the length it read from the TLV, is consistent with the actual length of data or not. If it isn’t shifts the return value by 0x80, which will trigger an error message at line 1184 of the outer function asn1\_check\_tlen in file tasn\_dec.c:  !!!  // In ASN1\_get\_object  if (\*plength > (omax - (p - \*pp))) {          ASN1err(ASN1\_F\_ASN1\_GET\_OBJECT, ASN1\_R\_TOO\_LONG);          /\*           \* Set this so that even if things are not long enough the values are           \* set correctly           \*/          ret |= 0x80;      }      \*pp = p;      return (ret | inf);  // In asn1\_check\_tlen  if (i & 0x80) {          ASN1err(ASN1\_F\_ASN1\_CHECK\_TLEN, ASN1\_R\_BAD\_OBJECT\_HEADER);          asn1\_tlc\_clear(ctx);          return 0;  For WolfSSL:  // Also reads in the length from TLV header but ignores it. This is fine for the initial SEQUENCE TLV, as there is a redundancy in place where WolfSSL checks for the input size and knows the certificate cannot exceed that, nor can it be smaller than that.  However, this is dangerous for the ASN.1 objects that are part of the initial SEQUENCE object as WolfSSL does not consider that the length can be tampered with, leading it to have a messed up translation from DER to its internal format, which results in data corruption.  // At line 2244 of GetCertHeader of file asn.c, the length from the TLV header is read in but is never taken into account and stored using internal format. Instead, the following lengths of the embedded ASN.1 SEQUENCE and BYTE STRING objects are actually stored and used as can be seen when cert->sigIndex = len + cert->srcIdx; is called, in order to get the length of the ASN.1 SEQUENCE object that is the first embedded structure within the entire SEQUENCE object that represents the whole certificate.  This results in only the index at which the certificate begins (start of initial SEQUENCE value) and the sigIndex, which should be the index of the certificate signature starting byte, are stored from the initial header.  if (GetSequence(cert->source, &cert->srcIdx, &len, cert->maxIdx) < 0)          return ASN\_PARSE\_E;      cert->certBegin = cert->srcIdx;      if (GetSequence(cert->source, &cert->srcIdx, &len, cert->maxIdx) < 0)          return ASN\_PARSE\_E;  cert->sigIndex = len + cert->srcIdx;  // While disregarding the initial len can be acceptable, as there is a redundancy in place (checking the length of the file) which makes the program know the max length possible of the certificate (maybe can be circumvented by using a abnormally large file size to make some kind of virus???), not ensuring that the following len is correct can be fatal, as it can displace the variable cert->sigIndex which is crucial in correctly checking the certificate. | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000001601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-16-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as ivptos 9, but with a different incorrect length | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000004701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-47-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as ivptos 9, but with a different incorrect length | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Most of the subsequent type 1 discrepancies occur because there is a known set structure to certificates sent in ASN.1 DER, as indicated by the following:    // Thus, wolfssl does not need to really consider the Tag and Length metadata as it was written with this structure in mind and does not need the metadata to guide its DER to internal translation process.  // Almost every single “discrepancy” between OpenSSL and WolfSSL is caused by this fact, where OpenSSL detects corruption in the Tag and Length data.  // I have a feeling that this can potentially be exploited since failure to detect corruption in the tag and length metadata of a TLV may lead to unexpected issues and translation problems, but if not, then WolfSSL can be considered to be actually better performing since it can disregard irrelevant errors and still accept a technically valid certificate  // For the following “discrepancies” that aren’t highlighted, the affected byte can be found in the wolfssl-openssl debug log, which will show that every one of them either belongs to the Tag or Length metadata. | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000011001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-110-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000011901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-119-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000013301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-133-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000013401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-134-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000014301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-143-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000014901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-149-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000015801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-158-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000019101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-191-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000019201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-192-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000023701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-237-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000023801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-238-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000023901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-239-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000024901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-249-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000517801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5178-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000531301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5313-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000541801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5418-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000544201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5442-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000544401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5444-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000541801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5418-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000544601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5446-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000547601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5476-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000548101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5481-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000548101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5489-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000549401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5494-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000549501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5495-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000549701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5497-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000549801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5498-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000550001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5500-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000554401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5544-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000564901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5649-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000567301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5673-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000567501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5675-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000567701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5677-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000570401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5704-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000567501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5675-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000567701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5677-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000570401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5704-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000570901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5709-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000571701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5717-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000572201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5722-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000572301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5723-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000572501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5725-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000572801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5728-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000577901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5779-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000588601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5886-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000591001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5910-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000591401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5914-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000594001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5940-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000594501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5945-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000595301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5953-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000595801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5958-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000595901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5959-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000596201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5962-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000596301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5963-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000596401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-5964-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000601701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6017-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000612401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6124-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000614801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6148-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000615001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6150-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/iid-0000615201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6152-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000617801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6178-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000618301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6183-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000619101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6191-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000619601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6196-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000619701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6197-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000619901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6199-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000620001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6200-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000670001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6700-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 224,225,226,227 // CA vs NULL | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000688401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6884-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 238 // MyOrg, Inc. // Printable string | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000688701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6887-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 239 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000689001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6890-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 240 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000689301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6893-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 241 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000689601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6896-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 242 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000689901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6899-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 243 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000690201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6902-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 244 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000690501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6905-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 245 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000690801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6908-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 246 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000691101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6911-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 247 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000691401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-6914-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 248 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000718001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7180-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 260 // mydomain.com // UTF8string | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000718301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7183-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 261 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000718601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7186-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 262 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000718901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7189-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 263 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000719201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7192-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 264 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000719501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7195-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 265 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000719801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7198-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 266 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000720101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7201-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 267 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000720401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7204-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 268 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000720701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7207-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 269 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000721001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7210-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 270 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000721301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-7213-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Bytes 271 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000806301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8063-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000807801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8078-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000810101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8101-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 282  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000810501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8105-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Byte 284  // Same as 8101 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000810701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8107-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Byte 285  // Same as 8101 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000820401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8204-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000824901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8249-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000844101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8441-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000848701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8487-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000853401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8534-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000863501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8635-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000877501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8775-subfuzz-1-dis-1.der  –  data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000889901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-8899-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000929301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9293-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 280  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000929901-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9299-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Bytes 288, 281, 282, 283, 284, 285, 286, 287  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000930201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9302-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 280  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000930301-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9303-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 280  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0000930601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-9306-subfuzz-1-dis-2.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Bytes 288, 281, 282, 283, 284, 285, 286, 287  // WolfSSL detects it but OpenSSL doesn’t?? | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001143601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11436-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 181 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001143701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11437-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 181 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001143801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11438-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 181 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001145601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11456-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 196 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001145701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11457-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 196 | |
| data/ssl/20220421\_165635\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-0\_all/testcases/id-0001145801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-11458-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| // UTC TIME is incorrect but WolfSSL is unable to detect it.  // Byte 196 | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000013801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-138-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000015601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-156-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000018201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-182-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000021001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-210-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000023701-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-237-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000026601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-266-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000029601-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-296-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000032001-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-320-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der  // Byte 126 | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000040401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-404-subfuzz-1-dis-1.der \*\*(Actual Data Corruption | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // UTC Time is incorrect but OpenSSL is unable to detect it  // 0x32 ( = 2) vs 0x2f (= /)  // Byte 186 | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000041501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-415-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000042801-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-428-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000045401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-454-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000048201-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-482-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000051101-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-511-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // See id-0000010401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-0-ivtpos-104-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000057401-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-574-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 280 - 282  // WolfSSL detects it but OpenSSL doesn’t | |
| data/ssl/20220421\_185749\_openssl-1.0.2h-wolfssl-3.9.6-update-1\_tgt-1\_all/testcases/id-1000057501-openssl-1.0.2h-wolfssl-3.9.6-update-1-tgt-1-ivtpos-575-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // OID is incorrect, should be {iso(1) member-body(2) us(840) rsadsi(113549)}  // Byte 280 - 282  // WolfSSL detects it but OpenSSL doesn’t | |

**Additional Info: IVTPOS 9/16/47**

Input Bytes for IVTPOS 9: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '01' instead of '04' and '46'

Input Bytes for IVTPOS 16: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '04' instead of '04' and '46'

Input Bytes for IVTPOS 47: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '0a' instead of '04' and '46'

|  |  |
| --- | --- |
| OpenSSL | WolfSSL |
|  | max == 5 != maxIdx == 1098 |

**Additional Info: IVTPOS 9/16/47**

Input Bytes for IVTPOS 9: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '01' instead of '04' and '46'

Input Bytes for IVTPOS 16: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '04' instead of '04' and '46'

Input Bytes for IVTPOS 47: Affected Byte at position 2, 3 (represents the length of the entire input): Is '00' and '0a' instead of '04' and '46'

|  |  |
| --- | --- |
| OpenSSL | WolfSSL |
| A computer screen shot of a program  Description automatically generated  A black screen with white text  Description automatically generated | A screenshot of a computer code  Description automatically generated  A computer screen shot of a program  Description automatically generated  max == 5 != maxIdx == 1098 |