**OpenSSL vs MbedTLS**

**Initial Remarks**

1. Development and Maintenance: OpenSSL has been around since 1998 and has a larger development community. It is maintained by the OpenSSL Software Foundation and receives contributions from various individuals and organizations. BoringSSL, on the other hand, is a fork of OpenSSL that was created by Google in 2014. It is specifically designed to be used internally by Google products, and its development is primarily driven by Google engineers.
2. Focus on Simplicity and Security: BoringSSL aims to be a minimalistic and simplified version of OpenSSL. It has a smaller codebase and a reduced feature set, focusing on providing only the essential cryptographic functions with a cleaner design. BoringSSL's goal is to improve code maintainability and security by minimizing the attack surface and reducing the risk of bugs and vulnerabilities.
3. API Compatibility: While BoringSSL started as a fork of OpenSSL, it has diverged significantly from the original codebase over time. BoringSSL introduced various API changes and removed certain legacy features and options present in OpenSSL. As a result, applications developed using OpenSSL may require modifications to work with BoringSSL.
4. Integration with Google Projects: BoringSSL has been optimized and tailored for Google's specific use cases and requirements. It has deeper integration with Google's software stack and is used in many Google products, such as Chrome, Android, and others. BoringSSL may include features and optimizations that are specific to Google's needs but not available in OpenSSL.
5. Licensing: OpenSSL historically used the OpenSSL License, which is considered to be permissive but has caused some licensing concerns in the past. BoringSSL, however, uses a more standard and simplified license called the "OpenSSL License," which is based on the Apache License 2.0. This change was made to address some of the licensing ambiguities and compatibility issues associated with the original OpenSSL License.

It's worth noting that while BoringSSL was initially intended for internal use at Google, it is open-source and can be used by others outside of Google. However, due to its more specialized nature, BoringSSL is generally recommended for projects closely tied to Google's ecosystem, while OpenSSL remains a widely adopted choice for general cryptographic needs in various applications and systems.

**Testcase Directories:**

1. 20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all
2. 20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all
3. 20220511\_171700\_openssl-1.0.2h-mbedtls-2.2.1-update-1-rank-1-71609\_tgt-0\_all
4. 20220511\_181310\_openssl-1.0.2h-mbedtls-2.2.1-update-1-rank-1-71609\_tgt-1\_all
5. 20220511\_184239\_openssl-1.0.2h-mbedtls-2.2.1-update-1-rank-2-c55ab\_tgt-0\_all
6. 20220511\_193626\_openssl-1.0.2h-mbedtls-2.2.1-update-1-rank-2-c55ab\_tgt-1\_all

|  |  |  |
| --- | --- | --- |
| @@ (path) | OpenSSL | MbedTLS |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as difference between OpenSSL and WolfSSL  // 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, MbedTLS 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 MbedTLS 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 MbedTLS 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 mbedtls-openssl debug log, which will show that every one of them either belongs to the Tag or Length metadata. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000041001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-410-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000042301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-423-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000046301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-463-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000046401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-464-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000047601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-476-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000064801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-648-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000064901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-649-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/iid-0000066201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-662-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000070201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-702-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000070301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-703-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000071501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-715-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000089001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-890-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000089101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-891-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000090401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-904-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000094201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-942-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000094301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-943-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000095501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-955-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000112801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1128-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000112901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1129-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000114201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1142-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000118501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1185-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000118601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1186-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000119801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1198-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000139101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1391-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000139201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1392-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000140501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1405-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000144601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1446-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000144701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1447-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000145901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1459-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000163201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1632-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000163301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1633-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000164601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1646-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000168901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1689-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000169001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1690-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000170201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1702-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000187601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1876-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000187701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1877-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000189001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1890-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000194301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1943-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000194401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-1944-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000521101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5211-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000521201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5212-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000522101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5221-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000541701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5417-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000541801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5418-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000543901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5439-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)} or 2.5.4.6 instead of 2.5.4.80  // Byte 209  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000544101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5441-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)} or 2.5.4.6 instead of 3.8.4.6  // Byte 207  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000544301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5443-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)} or 2.5.4.6 instead of 2.5.80.6  // Byte 208  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000564801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5648-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000564901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5649-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000567001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5670-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)} or 2.5.4.8 instead of 2.5.4.80  // Byte 222  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000567201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5672-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)} or 2.5.4.8 instead of 3.8.4.8  // Byte 220  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000567401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5674-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)} or 2.5.4.8 instead of 2.5.80.8  // Byte 221  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000588501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5885-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000588601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5886-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000590701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5907-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)} or 2.5.4.10 instead of 2.5.4.80  // Byte 235  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000590901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5909-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)} or 2.5.4.10 instead of 3.8.4.10  // Byte 233  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000591101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-5911-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)} or 2.5.4.10 instead of 2.5.80.10  // Byte 234  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000612301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6123-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000612401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6124-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000614501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6145-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)} or 2.5.4.3 instead of 2.5.4.80  // Byte 257  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000614701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6147-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)} or 2.5.4.3 instead of 3.8.4.3  // Byte 255  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000614901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6149-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // OID is incorrect, should be {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)} or 2.5.4.3 instead of 2.5.80.3  // Byte 256  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000669701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6697-subfuzz-1-dis-1.der\*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // State Name is incorrect, should be '43', '41' or ‘CA’ instead of ‘80', '51' or ‘S’ which MbedTLS still incorrectly accepts  // Valid state name identification is key to ensuring that either the issuer or subject is legitimate. The fact that MbedTLS is not able to recognize a corrupt State Name but OpenSSL is means there is a probable bug/vulnerability.  // OpenSSL detects it but MbedTLS does not | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000670001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6700-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as above (6697), except incorrect State Name should be '43', '41' or ‘CA’ instead of ‘20’, ‘80’ or ‘ ‘ | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000688401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6884-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Organization Name is incorrect, should be '4d', '79', '4f', '72', '67', '2c', '20', '49', '6e', '63', '2e' or ‘MyOrg, Inc.’, instead there is always a single corrupted Byte which MbedTLS still incorrectly accepts  // Valid organization name identification is key to ensuring that either the issuer or subject is legitimate. The fact that MbedTLS is not able to recognize a corrupt Org Name but OpenSSL is means there is a probable bug/vulnerability.  // First one is byte 238 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000688701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6887-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 239 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000689001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6890-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 240 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000689301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6893-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 241 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000689601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6896-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 242 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000689901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6899-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 243 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000690201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6902-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 244 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000690501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6905-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 245 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000690801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6908-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 246 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000691101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6911-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 247 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000691401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-6914-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 6884  // Byte 248 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000718001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7180-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Common Name is incorrect, should be '6d', '79', '64', '6f', '6d', '61', '69', '6e', '2e', '63', '6f', '6d' or ‘mydomain.com’, instead there is always a single corrupted Byte which MbedTLS still incorrectly accepts  // Valid Common Name identification is key to ensuring that either the issuer or subject is legitimate. The fact that MbedTLS is not able to recognize a corrupt CommonName but OpenSSL is able to means there is a probable bug/vulnerability.  // First one is byte 260 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000718301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7183-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 261 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000718601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7186-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 262 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000718901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7189-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 263 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000719201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7192-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 264 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000719501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7195-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 265 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000719801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7198-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 266 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000720101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7201-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 267 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000720401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7204-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 268 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000720701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7207-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 269 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000721001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7210-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 270 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000721301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-7213-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // Same as 7180  // Byte 271 | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000810101-openssl-1.0.2h-mbedtls-2.2.1-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1 instead of 1.2.1610726285.1.1.1  // Byte 282  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000810501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8105-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1 instead of 1.2.840.98317.1.1.1  // Byte 284  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000810701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8107-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1 instead of 1.2.840.116883457.1.1  // Byte 285  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000830801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-8308-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-0000040901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-409-subfuzz-1-dis-1.der  // Byte 579, wrong tag | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000929301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-9293-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1  // Byte 280  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000929901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-9299-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1  // Bytes 281,282,283,284,285,286,287,288  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000930201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-9302-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1  // Byte 280  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000930301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-9303-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1  // Byte 280  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_165933\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-0\_all/testcases/id-0000930601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-0-ivtpos-9306-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) pkcs(1) pkcs-1(1) rsaEncryption(1)} or 1.2.840.113549.1.1.1  // Bytes 281,282,283,284,285,286,287,288  // MbedTLS detects it but OpenSSL does not ??!? Major Bug since this involves the way the public key is hashed. | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der | Out: 0 | Out: 2 |
| Reason for Discrepancy:  // Similar to ivtpos 409, but it’s instead MbedTLS that is more strict with the Tags and Lengths of certain data types while OpenSSL is more forgiving.  // Something to note is that most of the data types that MbedTLS is more strict with have either tag ‘30’ which are Sequences (similar to data structures in C/C++) , tag ‘31’ which are Sets (similar to arrays in C/C++) or tag ‘16’ which are IA5 Strings  //On the other hand, OpenSSL is more strict with all the rest, such as tag ‘06’ which are OIDs, tag ‘02’ which are integers, tag ‘05’ which is NULL, tag ‘0c’ which are UTF8 Strings or tag ‘13’ which are Printable Strings.  // There are of course exceptions to the two above comments, and sometimes it’s random  // 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:  A screenshot of a computer code  Description automatically generated  // For the following “discrepancies” that aren’t highlighted, the affected byte can be found in the mbedtls-openssl debug log, which will show that every one of them either belongs to the Tag or Length metadata.  // This first one has byte 34 corrupted | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000005601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-56-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 37 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000007401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-74-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 46 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000008201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-82-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 50 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000010601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-106-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 63 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000013001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-130-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 81 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000015401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-154-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 96 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000017801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-178-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 110 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000020201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-202-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 126 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000021901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-219-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 141 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000022001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-220-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 141 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000022101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-221-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 141 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000023801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-238-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // UTC TIME is incorrect but OpenSSL is unable to detect it. This is probably due to the fact that the version of OpenSSL that PATHDIFF used on had not updated their UTC time check to ensure that only digits are allowed to be used. This results in corrupted bytes that are special characters and letters to be allowed by OpenSSL.  // ‘Before Time’ should be '32', '31', '30', '39', '32', '32', '31', '34', '33', '31', '30', '31', '5a' or 210922143101Z, instead, certain bytes are altered  // Byte 171 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000024001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-240-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 172 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000024201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-242-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 173 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000024401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-244-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 174 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000024601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-246-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 175 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000024801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-248-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 176 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-250-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 177 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-252-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 178 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-254-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 179 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-255-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 179 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-256-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 180 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-257-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 180 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000025901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-259-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 181 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000026001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-260-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 181 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000026101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-261-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 182 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000026201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-262-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 238, only different individual bytes of the UTC ‘Before Time’ String that are corrupted  // Byte 182 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-271-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // ‘After Time’ should be '32', '33', '30', '32', '30', '34', '31', '34', '33', '31', '30', '31', '5a' or 230204143101Z, instead, certain bytes are altered  // Byte 186 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-272-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 186 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-273-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 187 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-274-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 187 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-275-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 188 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-276-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 188 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-277-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 189 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-278-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 189 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000027901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-279-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 190 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-280-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 190 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-281-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 191 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-282-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 191 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-283-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 192 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-284-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 192 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-285-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 193 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-286-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 193 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-287-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 194 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-288-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 194 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000028901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-289-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 195 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000029001-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-290-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 195 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000029201-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-292-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 196 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000029301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-293-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 196 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000029401-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-294-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 197 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000029501-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-295-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Similar to ivtpos 271, only different individual bytes of the UTC ‘After Time’ String that are corrupted  // Byte 197 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000030101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-301-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 199 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000030701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-307-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 201 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000033301-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-333-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 214 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000035701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-357-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 227 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000038101-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-381-subfuzz-1-dis-1.der | Out: 2 | Out: 0 |
| Reason for Discrepancy:  // See id-1000004701-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-47-subfuzz-1-dis-1.der  // Byte 249 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000045801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-458-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Public Key Modulus is corrupted, major issue as this means the hash is incorrect and messages between server and client will not be encoded/decoded properly. OpenSSL does not detect this error, only MbedTLS does.  // Here are ways that OpenSSL should use to double check the legitimacy of the Public Key:  Signature Verification: The client verifies the digital signature of the certificate using the issuer's public key. If the signature verification fails due to the corrupted 'n', the certificate would be considered invalid.  Inconsistent Public Key Parameters: The client would expect the public key parameters (n, e) to match the parameters in the issuer's certificate. If the value of 'n' does not match, the client would detect the inconsistency.  Invalid RSA Modulus: RSA encryption and decryption operations depend on the proper modulus 'n'. If the 'n' value is incorrect, encryption and decryption operations would yield incorrect results, which could be detected during the handshake process.  Certificate Chain Validation: The certificate chain is also validated to ensure that each certificate in the chain is signed by the appropriate issuer. Any modification to the public key or certificate would likely break the chain validation.  // This is right after an OID identifying that this is a Public key at Byte 278: '2a', '86', '48', '86', 'f7', '0d', '01', '01', '01' or {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}  // Byte 305 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000072601-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-726-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Public Key Public Exponent is corrupted, again results in major issue as this means the hash is incorrect and messages between server and client will not be encoded/decoded properly. OpenSSL does not detect this error, only MbedTLS does.  // This proves that OpenSSL does not properly check public key validity and assumes everything is fine after checking subject, issuer and dates, which can be a major issue. This is however probably already fixed since the OpenSSL version that is being tested on is not up-to-date. Not confirmed though, easiest way would be to simply give this input to the newest version of OpenSSL and see if it detects a problem. If it doesn’t then the vulnerability still exists.  // Byte 563 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000073801-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-738-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Same as ivtpos 458, only for different modulus bytes  // Bytes 553,554,555,556,557,558,559,560 | |
| data/ssl/20220421\_174951\_openssl-1.0.2h-mbedtls-2.2.1-update-1\_tgt-1\_all/testcases/id-1000073901-openssl-1.0.2h-mbedtls-2.2.1-update-1-tgt-1-ivtpos-739-subfuzz-1-dis-1.der \*\*(Actual Data Corruption) | Out: 0 | Out: 2 |
| // Same as ivtpos 458, only for different modulus bytes  // Bytes 553,554,555,556,557,558,559,560 | |