New issue

Jump to bottom

Lack of encoding checking in jsrsasign allows a certain degree of malleability in ECDSA signatures #437

Closed **adelapie** opened this issue on Jun 6, 2020 · 2 comments

Labels bug

adelapie commented on Jun 6, 2020

Hello,

I've found that jsrsasign 8.0.16 allows a certain degree of malleability in ECDSA signatures by
not checking overflows in the length of sequence and 0s appended or prepended to an integer.

Using the secp256r1 curve it its possible to verify this issue using the following test vectors of Google Wycheproof:


```
{
  "algorithm" : "ECDSA",
  "generatorVersion" : "0.8r12",
  "numberOfTests" : 387,
  "header" : [
    "Test vectors of type EcdsaVerify are meant for the verification",
    "of ASN encoded ECDSA signatures."
  ],
  "notes" : {
    "BER" : "This is a signature with correct values for (r, s) but using some alternative BER encoding instead of DER encoding. Implementations should not accept such signatures
to limit signature malleability.",
    "EdgeCase" : "Edge case values such as r=1 and s=0 can lead to forgeries if the ECDSA implementation does not check boundaries and computes s^(-1)==0.",
    "MissingZero" : "Some implementations of ECDSA and DSA incorrectly encode r and s by not including leading zeros in the ASN encoding of integers when necessary. Hence, some
implementations (e.g. jdk) allow signatures with incorrect ASN encodings assuming that the signature is otherwise valid.",
    "PointDuplication" : "Some implementations of ECDSA do not handle duplication and points at infinity correctly. This is a test vector that has been specially crafted to check
for such an omission."
  },
  "schema" : "ecdsa_verify_schema.json",
  "testGroups" : [
    {
      "key" : {
        "curve" : "secp256r1",
        "keySize" : 256,
        "type" : "EcPublicKey",
        "uncompressed" : "042927b10512bae3eddcfe467828128bad2903269919f7086069c8c4df6c732838c7787964eaac00e5921fb1498a60f4606766b3d9685001558d1a974e7341513e",
        "wx" : "2927b10512bae3eddcfe467828128bad2903269919f7086069c8c4df6c732838",
        "wy" : "00c7787964eaac00e5921fb1498a60f4606766b3d9685001558d1a974e7341513e"
      },
      "keyDer" :
"3059301306072a8648ce3d020106082a8648ce3d03010703420042927b10512bae3eddcfe467828128bad2903269919f7086069c8c4df6c732838c7787964eaac00e5921fb1498a60f4606766b3d9685001558d1a974e7341513e
      "keyPem" : "-----BEGIN PUBLIC KEY-----\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEKSexBRK64+3c/kZ4KBKLrSkDJpkZ\n9whgacjE32xzKDjHeHlk6qwA5ZIfsUmKYPRgZ2az2WhQAVWNGpdOc0FRPg==\n-----
END PUBLIC KEY-----",
      "sha" : "SHA-256",
      "type" : "EcdsaVerify",
      "tests" : [
        {
          "tcId" : 1,
          "comment" : "signature malleability",
          "msg" : "313233343030",
          "sig" : "304402202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802204cd60b855d442f5b3c7b11eb6c4e0ae7525fe710fab9aa7c77a67f79e6fadd76",
          "result" : "valid",
          "flags" : []
        },
        {
          "tcId" : 2,
          "comment" : "Legacy:ASN encoding of s misses leading 0",
          "msg" : "313233343030",
          "sig" : "304402202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180220b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "acceptable",
          "flags" : [
            "MissingZero"
          ]
        },
        {
          "tcId" : 3,
          "comment" : "valid",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "valid",
          "flags" : []
        },
        {
          "tcId" : 4,
          "comment" : "long form encoding of length of sequence",
          "msg" : "313233343030",
          "sig" : "30814502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 5,
          "comment" : "length of sequence contains leading 0",
          "msg" : "313233343030",
          "sig" : "3082004502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 6,
          "comment" : "wrong length of sequence",
          "msg" : "313233343030",
          "sig" : "304602202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 7,
          "comment" : "wrong length of sequence",
          "msg" : "313233343030",
          "sig" : "304402202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 8,
          "comment" : "uint32 overflow in length of sequence",
          "msg" : "313233343030",
          "sig" : "3085010000004502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
```

```
        },
        {
          "tcId" : 9,
          "comment" : "uint64 overflow in length of sequence",
          "msg" : "313233343030",
          "sig" :
"308901000000000000004502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 10,
          "comment" : "length of sequence = 2**31 - 1",
          "msg" : "313233343030",
          "sig" : "30847fffffff02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 11,
          "comment" : "length of sequence = 2**32 - 1",
          "msg" : "313233343030",
          "sig" : "3084ffffffff02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 12,
          "comment" : "length of sequence = 2**40 - 1",
          "msg" : "313233343030",
          "sig" : "3085ffffffffff02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 13,
          "comment" : "length of sequence = 2**64 - 1",
          "msg" : "313233343030",
          "sig" : "3088ffffffffffffffff02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 14,
          "comment" : "incorrect length of sequence",
          "msg" : "313233343030",
          "sig" : "30ff02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 15,
          "comment" : "indefinite length without termination",
          "msg" : "313233343030",
          "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 16,
          "comment" : "indefinite length without termination",
          "msg" : "313233343030",
          "sig" : "304502802ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 17,
          "comment" : "indefinite length without termination",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18028000b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 18,
          "comment" : "removing sequence",
          "msg" : "313233343030",
          "sig" : "",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 19,
          "comment" : "lonely sequence tag",
          "msg" : "313233343030",
          "sig" : "30",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 20,
          "comment" : "appending 0's to sequence",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 21,
          "comment" : "prepending 0's to sequence",
          "msg" : "313233343030",
          "sig" : "3047000002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 22,
          "comment" : "appending unused 0's to sequence",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
          "result" : "invalid",
          "flags" : []
```

```
},
{
  "tcId" : 23,
  "comment" : "appending null value to sequence",
  "msg" : "313233343030",
  "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0500",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 24,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304a498177304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 25,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "30492500304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 26,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "3047304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0004deadbeef",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 27,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304a222549817702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 28,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "30492224250002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 29,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304d222202202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180004deadbeef022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 30,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304a02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1822264981770221 00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 31,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304902202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1822252500022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 32,
  "comment" : "including garbage",
  "msg" : "313233343030",
  "sig" : "304d02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e182223022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0004deadbeef",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 33,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304daa00bb00cd00304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 34,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304baa02aabb304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 35,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304d2228aa00bb00cd0002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 36,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304b2226aa02aabb02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
```

```
{
  "tcId" : 37,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304d02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e182229aa00bb00cd00022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 38,
  "comment" : "including undefined tags",
  "msg" : "313233343030",
  "sig" : "304b02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e182227aa02aabb022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 39,
  "comment" : "truncated length of sequence",
  "msg" : "313233343030",
  "sig" : "3081",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 40,
  "comment" : "using composition with indefinite length",
  "msg" : "313233343030",
  "sig" : "3080304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 41,
  "comment" : "using composition with indefinite length",
  "msg" : "313233343030",
  "sig" : "3049228002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180000022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 42,
  "comment" : "using composition with indefinite length",
  "msg" : "313233343030",
  "sig" : "304902202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e182280022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 43,
  "comment" : "using composition with wrong tag",
  "msg" : "313233343030",
  "sig" : "3080314502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 44,
  "comment" : "using composition with wrong tag",
  "msg" : "313233343030",
  "sig" : "3049228003202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180000022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 45,
  "comment" : "using composition with wrong tag",
  "msg" : "313233343030",
  "sig" : "304902202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e182280032100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 46,
  "comment" : "Replacing sequence with NULL",
  "msg" : "313233343030",
  "sig" : "0500",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 47,
  "comment" : "changing tag value of sequence",
  "msg" : "313233343030",
  "sig" : "2e4502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 48,
  "comment" : "changing tag value of sequence",
  "msg" : "313233343030",
  "sig" : "2f4502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 49,
  "comment" : "changing tag value of sequence",
  "msg" : "313233343030",
  "sig" : "314502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
  "tcId" : 50,
  "comment" : "changing tag value of sequence",
  "msg" : "313233343030",
  "sig" : "324502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
  "result" : "invalid",
  "flags" : []
},
{
```

```
    "tcId" : 51,
    "comment" : "changing tag value of sequence",
    "msg" : "313233343030",
    "sig" : "ff4502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 52,
    "comment" : "dropping value of sequence",
    "msg" : "313233343030",
    "sig" : "3000",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 53,
    "comment" : "using composition for sequence",
    "msg" : "313233343030",
    "sig" : "3049300102304420 2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 54,
    "comment" : "truncated sequence",
    "msg" : "313233343030",
    "sig" : "304402202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 55,
    "comment" : "truncated sequence",
    "msg" : "313233343030",
    "sig" : "3044202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 56,
    "comment" : "indefinite length",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
    "result" : "invalid",
    "flags" : [
      "BER"
    ]
  },
  {
    "tcId" : 57,
    "comment" : "indefinite length with truncated delimiter",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db00",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 58,
    "comment" : "indefinite length with additional element",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db05000000",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 59,
    "comment" : "indefinite length with truncated element",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db060811220000",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 60,
    "comment" : "indefinite length with garbage",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000fe02beef",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 61,
    "comment" : "indefinite length with nonempty EOC",
    "msg" : "313233343030",
    "sig" : "308002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0002beef",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 62,
    "comment" : "prepend empty sequence",
    "msg" : "313233343030",
    "sig" : "3047300002202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 63,
    "comment" : "append empty sequence",
    "msg" : "313233343030",
    "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db3000",
    "result" : "invalid",
    "flags" : []
  },
  {
    "tcId" : 64,
    "comment" : "append garbage with high tag number",
    "msg" : "313233343030",
    "sig" : "304802202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847dbbf7f00",
    "result" : "invalid",
    "flags" : []
  },
```

```
        {
          "tcId" : 65,
          "comment" : "sequence of sequence",
          "msg" : "313233343030",
          "sig" : "3047304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 66,
          "comment" : "truncated sequence: removed last 1 elements",
          "msg" : "313233343030",
          "sig" : "302202202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 67,
          "comment" : "repeating element in sequence",
          "msg" : "313233343030",
          "sig" :
"306802202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db022100b329f479a2bbd0a5c384ee1493b1f5186a
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 68,
          "comment" : "long form encoding of length of integer",
          "msg" : "313233343030",
          "sig" : "30460281202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 69,
          "comment" : "long form encoding of length of integer",
          "msg" : "313233343030",
          "sig" : "304602202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802812100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 70,
          "comment" : "length of integer contains leading 0",
          "msg" : "313233343030",
          "sig" : "3047028200202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 71,
          "comment" : "length of integer contains leading 0",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180282002100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 72,
          "comment" : "wrong length of integer",
          "msg" : "313233343030",
          "sig" : "304502212ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 73,
          "comment" : "wrong length of integer",
          "msg" : "313233343030",
          "sig" : "3045021f2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 74,
          "comment" : "wrong length of integer",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022200b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 75,
          "comment" : "wrong length of integer",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022000b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 76,
          "comment" : "uint32 overflow in length of integer",
          "msg" : "313233343030",
          "sig" : "304a028501000000202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 77,
          "comment" : "uint32 overflow in length of integer",
          "msg" : "313233343030",
          "sig" : "304a02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802850100000002100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
```

```
        {
          "tcId" : 78,
          "comment" : "uint64 overflow in length of integer",
          "msg" : "313233343030",
          "sig" :
"304e02890100000000000000202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 79,
          "comment" : "uint64 overflow in length of integer",
          "msg" : "313233343030",
          "sig" :
"304e02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802890100000000000000002100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 80,
          "comment" : "length of integer = 2**31 - 1",
          "msg" : "313233343030",
          "sig" : "304902847fffffff2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 81,
          "comment" : "length of integer = 2**31 - 1",
          "msg" : "313233343030",
          "sig" : "304902202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802847fffffff00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 82,
          "comment" : "length of integer = 2**32 - 1",
          "msg" : "313233343030",
          "sig" : "30490284ffffffff2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 83,
          "comment" : "length of integer = 2**32 - 1",
          "msg" : "313233343030",
          "sig" : "304902202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180284ffffffff00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 84,
          "comment" : "length of integer = 2**40 - 1",
          "msg" : "313233343030",
          "sig" : "304a0285fffffffff2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 85,
          "comment" : "length of integer = 2**40 - 1",
          "msg" : "313233343030",
          "sig" : "304a02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180285fffffffff00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 86,
          "comment" : "length of integer = 2**64 - 1",
          "msg" : "313233343030",
          "sig" : "304d0288ffffffffffffffff2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 87,
          "comment" : "length of integer = 2**64 - 1",
          "msg" : "313233343030",
          "sig" : "304d02202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180288ffffffffffffffff00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 88,
          "comment" : "incorrect length of integer",
          "msg" : "313233343030",
          "sig" : "304502ff2ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 89,
          "comment" : "incorrect length of integer",
          "msg" : "313233343030",
          "sig" : "304502202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802ff00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 90,
          "comment" : "removing integer",
          "msg" : "313233343030",
          "sig" : "3023022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 91,
          "comment" : "lonely integer tag",
          "msg" : "313233343030",
          "sig" : "3024020221 00b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
```

```
        },
        {
          "tcId" : 92,
          "comment" : "lonely integer tag",
          "msg" : "313233343030",
          "sig" : "302302202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e1802",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 93,
          "comment" : "appending 0's to integer",
          "msg" : "313233343030",
          "sig" : "304702222ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180000022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 94,
          "comment" : "appending 0's to integer",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022300b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0000",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 95,
          "comment" : "prepending 0's to integer",
          "msg" : "313233343030",
          "sig" : "3047022200002ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 96,
          "comment" : "prepending 0's to integer",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180223000000b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : [
            "BER"
          ]
        },
        {
          "tcId" : 97,
          "comment" : "appending unused 0's to integer",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180000022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 98,
          "comment" : "appending null value to integer",
          "msg" : "313233343030",
          "sig" : "304702222ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e180500022100b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db",
          "result" : "invalid",
          "flags" : []
        },
        {
          "tcId" : 99,
          "comment" : "appending null value to integer",
          "msg" : "313233343030",
          "sig" : "304702202ba3a8be6b94d5ec80a6d9d1190a436effe50d85a1eee859b8cc6af9bd5c2e18022300b329f479a2bbd0a5c384ee1493b1f5186a87139cac5df4087c134b49156847db0500",
          "result" : "invalid",
          "flags" : []
        }
      ]
    }
  ]
}
```

```
var rs = require('jsrsasign');
var obj = require("./poc_ecdsa_secp256r1_sha256_test.json");

for (let testGroup of obj.testGroups) {

    var keyPem = testGroup.keyPem;

    for(let test of testGroup.tests) {
     console.log("[*] Test " + test.tcId + " result: " + test.result)

     try {
      var sig = new rs.Signature({alg: 'SHA256withECDSA'});
      sig.init(keyPem);

      sig.updateHex(test.msg);
      var result = sig.verify(test.sig);

     if (result == true) {
      if (test.result == "valid" || test.result == "acceptable")
       console.log("Result: PASS");
      else
       console.log("Result: FAIL")
     }

     if (result == false) {
      if (test.result == "valid" || test.result == "acceptable")
       console.log("Result: FAIL");
      else
       console.log("Result: PASS")
```

```
      }

      } catch (e) {
       console.log("ERROR - VERIFY: " + e)

       if (test.result == "valid" || test.result == "acceptable")
        console.log("Result: FAIL");
       else
        console.log("Result: PASS")

      }

     }
  }
```

The output is:

```
  [*] Test 4 result: invalid
  Result: FAIL
  [*] Test 5 result: invalid
  Result: FAIL
  [*] Test 7 result: invalid
  Result: FAIL
  [*] Test 8 result: invalid
  Result: FAIL
  [*] Test 9 result: invalid
  Result: FAIL
  [*] Test 22 result: invalid
  Result: FAIL
  [*] Test 68 result: invalid
  Result: FAIL
  [*] Test 69 result: invalid
  Result: FAIL
  [*] Test 70 result: invalid
  Result: FAIL
  [*] Test 71 result: invalid
  Result: FAIL
  [*] Test 74 result: invalid
  Result: FAIL
  [*] Test 76 result: invalid
  Result: FAIL
  [*] Test 77 result: invalid
  Result: FAIL
  [*] Test 78 result: invalid
  Result: FAIL
  [*] Test 79 result: invalid
  Result: FAIL
  [*] Test 81 result: invalid
  Result: FAIL
  [*] Test 89 result: invalid
  Result: FAIL
  [*] Test 95 result: invalid
  Result: FAIL
  [*] Test 96 result: invalid
  Result: FAIL
```

However, if you use node.js crypto:

```
  const crypto = require('crypto');

  var obj = require("./poc_ecdsa_secp256r1_sha256_test.json");

  for (let testGroup of obj.testGroups) {
      keyPem = testGroup.keyPem;

      for(let test of testGroup.tests) {
       console.log("[*] Test " + test.tcId + " result: " + test.result)

       var verifier = crypto.createVerify('SHA256');
       verifier.update(Buffer.from(test.msg, 'hex'));
       var result = (verifier.verify(keyPem, Buffer.from(test.sig, 'hex')))

       if (result == true) {
        if (test.result == "valid" || test.result == "acceptable")
         console.log("Result: PASS");
        else
         console.log("Result: FAIL")
       }

       if (result == false) {
        if (test.result == "valid" || test.result == "acceptable")
         console.log("Result: FAIL");
        else
         console.log("Result: PASS")
       }

      }

  }
```

the output is:

```
  [*] Test 4 result: invalid
  Result: PASS
  [*] Test 5 result: invalid
  Result: PASS
  [*] Test 7 result: invalid
  Result: PASS
  [*] Test 8 result: invalid
  Result: PASS
  [*] Test 9 result: invalid
  Result: PASS
  [*] Test 22 result: invalid
  Result: PASS
```

```
[*] Test 68 result: invalid
Result: PASS
[*] Test 69 result: invalid
Result: PASS
[*] Test 70 result: invalid
Result: PASS
[*] Test 71 result: invalid
Result: PASS
[*] Test 74 result: invalid
Result: PASS
[*] Test 76 result: invalid
Result: PASS
[*] Test 77 result: invalid
Result: PASS
[*] Test 78 result: invalid
Result: PASS
[*] Test 79 result: invalid
Result: PASS
[*] Test 81 result: invalid
Result: PASS
[*] Test 89 result: invalid
Result: PASS
[*] Test 95 result: invalid
Result: PASS
[*] Test 96 result: invalid
Result: PASS
```

Best regards,
Antonio

kjur commented on Jun 22, 2020 — Owner

Thank you for your report. This issue was fixed in the 8.0.19 release today.

kjur closed this as completed on Jun 22, 2020

---

kjur commented on Jun 23, 2020 — Owner

Security advisory is published for this:

jsrsasign security advisory (2020-Jun-24):
CVE-2020-14966
ECDSA signature validation vulnerability by accepting wrong ASN.1 encoding
GHSA-p8c3-7rj8-q963

kjur added the bug label on Aug 24, 2020

This was referenced on Mar 13, 2021

Bump jsrsasign from 8.0.12 to 8.0.19 m0rphtail/Teleport#6
Closed

Bump jsrsasign from 8.0.12 to 8.0.19 Cyper77/CyberChef#1
Closed

Assignees
No one assigned

Labels
bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants