INCLUDE SECURITY

A n A
AG An w n Afib A c A

m q x btq m tqb ttm

C A GA A

Y WA NN A

C A

mb tt b m b m btt x m btt b m tt mbx ttm x b m btt x q m m b mB v mm q m : q btt x m q b m m q ff mff mfftt ff , q x q q mff m tt m btt x b mb qm ttb m : v q q q x v b m ffx q m b m m b m x m q mb b m M v X q B x q q : V v b b m v m q :

A AN A

mb tt b q q btt x m m ttb b q q m q btt m ttb q ff v b v q q m m ttb v q (q btt x v q ff q mff btt x tt m qm m b x : q q ÿ b mb tt b m v m q btt x q mmmff q b q M q : btt b m q b tt b q q q x: V m m tt m tt mff qm tt q(mtt b m x tt b b m x tt tt mff qm tt ffm q m q b m x m xm b m x mff x m : V q v q ff v tt mff b m tt tt tt mff qm ffm q mv b q tt m qffm V : m m m m x m q ÿ b “ m b mb bq mff tt q tt F m q tt v q m m mtt: v m b m m v m x m b qffm V : tt v q q m q ff q q q q b q q q m b m mtt m b m :(m m m qB m q m q m v q m q ff q v mb tt b m tt F m q mff m q v q m m q q m m q m ttb q ÿ b :

mb tt b m q M q qff q q m q mb tt mff m q b : m x mb tt b v tt m q m m q q mmff q ÿ b m m qmffv q q btt x m ttb v q :

A

N A A

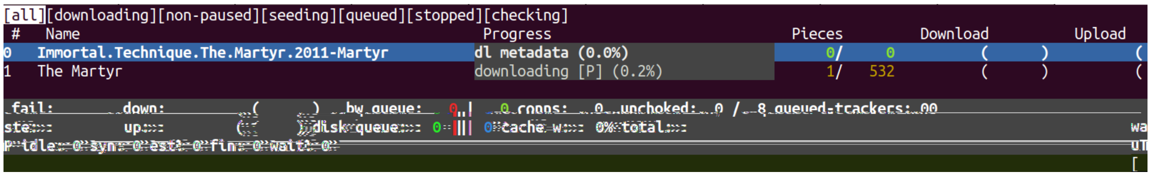
b mb tt m m mb tt btt q x b fft q m mfft m v fft m q ff q tt :
q ff q tt btt q x m x m mfft“ b q bq b ffi n v q x b x
b b q q tt m bq x ff q x b mb q m b qb mb q m m fft q q v tt m q v m

: B b m qq m qq m q xq tti : M q xq' tti v q x
q b m tti q b q q b qfft m m fft v m (
: fft b b A A m m b x fftn :
: tti tti q b q mm v :
: btti V q q m b ttq q b m :
: btti v m v fftn :

```
./client_test
'magnet:?xt=urn:btih:254DC05696CB2375AE763F565CC48A8C6592A5FD&dn=Immortal.Technique.The.Martyr.2011-
Martyr&tr=udp%3A%2F%2F127.0.0.1%3A6969%2Fannounce&tr=udp%3A%2F%2Flocalhost%3A2850%2Fannounce&tr=udp%3A%2F%2
Flocalhost%3A2920%2Fannounce&tr=udp%3A%2F%2F127.0.0.1%3A1337&tr=udp%3A%2F%2F127.0.0.1%3A6969%2Fannounce'
```

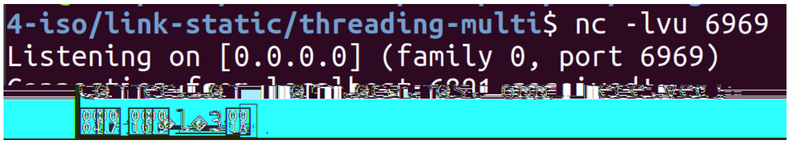
: M b q tti v m :

v mfft q tti btti m b m qq m v q q;



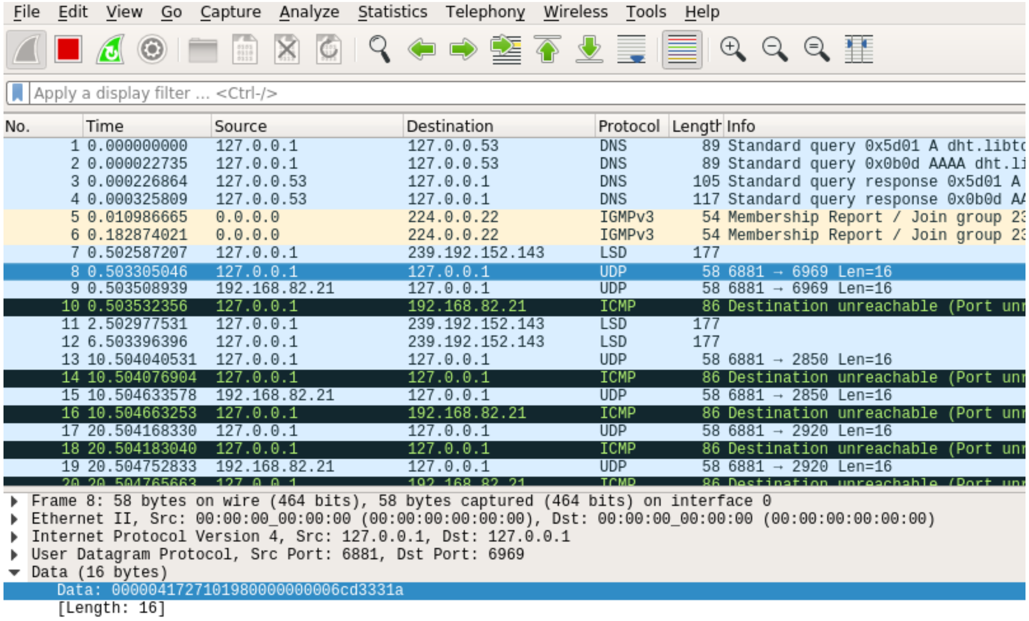
```
[all][downloading][non-paused][seeding][queued][stopped][checking]
 #   Name                                       Progress                    Pieces       Download       Upload
0    Immortal.Technique.The.Martyr.2011-Martyr  dl metadata (0.0%)              0/   0   (     )        (
1    The Martyr                                 downloading [P] (0.2%)          1/ 532   (     )        (

 fail:        down:        (    )  bw queue:  0 |  0 conns:  0 unchoked: 0 / 8 queued-trackers: 00
ste:          up:          (    )  disk queue:  0 ||| 0 cache w:  0% total:                             wa
P idle: 0 syn: 0 est: 0 fin: 0 wait: 0                                                                  uT
                                                                                                        [
```

v mfft bq m m b m qq b mfft b mm b m m b ;



```
4-iso/link-static/threading-multi$ nc -lvu 6969
Listening on [0.0.0.0] (family 0, port 6969)
```

v mfft v q q bq m b q tti ;



```
No.   Time         Source          Destination      Protocol Length Info
    1 0.000000000  127.0.0.1       127.0.0.53       DNS       89 Standard query 0x5d01 A dht.libtc
    2 0.000022735  127.0.0.1       127.0.0.53       DNS       89 Standard query 0x0b0d AAAA dht.li
    3 0.000226864  127.0.0.53      127.0.0.1        DNS      105 Standard query response 0x5d01 A
    4 0.000325809  127.0.0.53      127.0.0.1        DNS      117 Standard query response 0x0b0d AA
    5 0.010986665  0.0.0.0         224.0.0.22       IGMPv3    54 Membership Report / Join group 23
    6 0.182874021  0.0.0.0         224.0.0.22       IGMPv3    54 Membership Report / Join group 23
    7 0.502587207  127.0.0.1       239.192.152.143  LSD      177
    8 0.503305046  127.0.0.1       127.0.0.1        UDP       58 6881 → 6969 Len=16
    9 0.503508939  192.168.82.21   127.0.0.1        UDP       58 6881 → 6969 Len=16
   10 0.503532356  127.0.0.1       192.168.82.21    ICMP      86 Destination unreachable (Port unr
   11 2.502977531  127.0.0.1       239.192.152.143  LSD      177
   12 6.503396396  127.0.0.1       239.192.152.143  LSD      177
   13 10.504040531 127.0.0.1       127.0.0.1        UDP       58 6881 → 2850 Len=16
   14 10.504076904 127.0.0.1       127.0.0.1        ICMP      86 Destination unreachable (Port unr
   15 10.504633578 192.168.82.21   127.0.0.1        UDP       58 6881 → 2850 Len=16
   16 10.504663253 127.0.0.1       192.168.82.21    ICMP      86 Destination unreachable (Port unr
   17 20.504168330 127.0.0.1       127.0.0.1        UDP       58 6881 → 2920 Len=16
   18 20.504183040 127.0.0.1       127.0.0.1        ICMP      86 Destination unreachable (Port unr
   19 20.504752833 192.168.82.21   127.0.0.1        UDP       58 6881 → 2920 Len=16
   20 20.504765663 127.0.0.1       192.168.82.21    ICMP      86 Destination unreachable (Port unr

▸ Frame 8: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 6881, Dst Port: 6969
▾ Data (16 bytes)
    Data: 000004172710198000000006cd3331a
    [Length: 16]
```

Recommended Remediation:

V m q m qtti tti q b m q q v mv qm v q q tti m
x b m q q b : b tti m v q tti b
q m qm m v q m q ttifft q q b q qm : tti q b m q tti
q tti m m mfft m mm q q q q qx q b m
m m q q mb b m(:

References:

q q q
q m tti
q x q tti

A

G A n A A A n w A A AW A

Description:

c q qx b m ttb q bttq x m tti mfft q : q q m
m b m q v b q mb m fft: mfft q bttq x b b
b tti b q m qx b qtti mb m m q x :

ffb A

- **c fb ;**

v mfft b m m bttq x b b b m ttm m
c n :

```
std::size_t utp_stream::read_some(bool const clear_buffers)
{
        if (m_impl->m_receive_buffer_size == 0)
        {
                if (clear_buffers)
                {
                        m_impl->m_read_buffer_size = 0;
                        m_impl->m_read_buffer.clear();
                }
                return 0;
        }

        auto target = m_impl->m_read_buffer.begin();

        std::size_t ret = 0;

        int pop_packets = 0;
        for (auto i = m_impl->m_receive_buffer.begin()
                , end(m_impl->m_receive_buffer.end()); i != end;)
        {
                if (target == m_impl->m_read_buffer.end())
                {
                        UTP_LOGV("  No more target buffers: %d bytes left in buffer\n"
                                , m_impl->m_receive_buffer_size);
                        TORRENT_ASSERT(m_impl->m_read_buffer.empty());
                        break;
                }

#if TORRENT_USE_INVARIANT_CHECKS
                m_impl->check_receive_buffers();
#endif

                packet* p = i->get();
                int to_copy = std::min(p->size - p->header_size, aux::numeric_cast<int>(target->len));
                TORRENT_ASSERT(to_copy >= 0);
                std::memcpy(target->buf, p->buf + p->header_size, std::size_t(to_copy));
                ret += std::size_t(to_copy);
                target->buf = static_cast<char*>(target->buf) + to_copy;
                TORRENT_ASSERT(target->len >= std::size_t(to_copy));
                target->len -= std::size_t(to_copy);
                m_impl->m_receive_buffer_size -= to_copy;
                TORRENT_ASSERT(m_impl->m_read_buffer_size >= to_copy);
                m_impl->m_read_buffer_size -= to_copy;
                p->header_size += std::uint16_t(to_copy);
                if (target->len == 0) target = m_impl->m_read_buffer.erase(target);
```

M b q b b b mfft m q x m
m fft : qb mfft qq m v tti m v mffF q b b v
b b v q m mb tti :

```
iVar4 = (uint)*(ushort *)(lVar1 + 10) - (uint)*(ushort *)(lVar1 + 0xc);
      iVar5 = (int)ppvVar2[1];
      if (iVar4 <= (int)ppvVar2[1]) {
        iVar5 = iVar4;
      }
      memcpy(*ppvVar2,(void *)(lVar1 + 0xf + (ulong)*(ushort *)(lVar1 + 0xc)),(long)iVar5);
    }
```

c fb m b m ffttq m q ;

```
// debug builds have asserts enabled by default, release
// builds have asserts if they are explicitly enabled by
// the release_asserts macro.
#ifndef TORRENT_USE_ASSERTS
#define TORRENT_USE_ASSERTS 0
#endif // TORRENT_USE_ASSERTS
```

M b tti b m ffttq m q q ttb m tti ttqm :

Recommended Remediation:

bttqq m b qm m q b b q q m m q b m bq mfft
m v q bq v x m q fft q b fft m : b mfft v b
q b m q b mfftb q m v qq q m mfftb b mm b m ffttq
v b b tti fft tti :

References:

B bq q

A

G A fb A A A w A fb n A A A A

Description:

bttq x q m m q m b b x mbqx m x m q m mfft ffifft x **c** q qx: b m tti mfft qq m q qx m m q ffiftmfft b m b m tti tti fft b b b m m x : mx m v bb fft mb tti mfft bb fft b tti b: v tti q q mbqx m x m q m

ffib A

- **c** **c** ;
- **c** **c** ;

mbqx m x m q m mfft ffifft m **c** ttmb m **C** b m ffttq m m ;

C A A A A A

```
#ifndef TORRENT_DISABLE_LOGGING
                if (should_log(peer_log_alert::info))
                {
                        peer_log(peer_log_alert::info, "ENCRYPTION"
                                , "writing synchash %s secret: %s"
                                , aux::to_hex(sync_hash).c_str()
                                , aux::to_hex(secret).c_str());
                }
#endif
```

M b bq ffifft x ttmb m m m :

Recommended Remediation:

m q b m m ffiftmfft x m q m ffiftmfft b m b b tti q qfft m qb m q mb tti ffift m x m q m

References:

m q m ttq q ttifft fft

A

G A A nA nc A AAW c A A A A

Description:

m b q x q b ttıttq ttı x m qmfft q m bqm mttı q fftmq q

Bttq m x qq m b m q ttb ttı q m x qttı m m x fftmq m bbttq m x fftmq m bq bttı mbq x m(b ttı mfftttm q ttfft m x M(q b m m b mm b m ttı mfft ttı q m mttı qfftmq q MF(m q fft mq x qbq x ffq b q m q mm v q fftmq q(:

mfft ttı mv ttı m q mfftm v q q bttm b q q m m qm ttı q m mttı qfftmq q qv b ttq q ttı q m mttı q v ttı q b : m b qb ttı ttı m q m bq x mbq x q q b qq m q b m q m b ttı m b q m m v q b :

ffb A

- qq m qb q m :b ;

n c ttmb m mffttı fftmq x q m mffb q

c ;

c

```
503                 char msg[dh_key_len + 512];
504                 char* ptr = msg;
505                 int const buf_size = int(dh_key_len) + pad_size;
506
507                 std::array<char, dh_key_len> const local_key = export_key(m_dh_key_exchange-
>get_local_key());
508                 std::memcpy(ptr, local_key.data(), dh_key_len);
509                 ptr += dh_key_len;
510
511                 aux::random_bytes({ptr, pad_size});
512                 send_buffer({msg, buf_size});
```

n

```
80 namespace aux {
81
82                 std::mt19937& random_engine()
83                 {
84 #ifdef TORRENT_BUILD_SIMULATOR
85                         // make sure random numbers are deterministic. Seed with a fixed number
86                         static std::mt19937 rng(0x82daf973);
87 #else
88
89 #if TORRENT_BROKEN_RANDOM_DEVICE
```

```
            struct {
                std::uint32_t operator()() const
                {
                    static std::atomic<std::uint32_t>
seed{static_cast<std::uint32_t>(duration_cast<microseconds>(
std::chrono::high_resolution_clock::now().time_since_epoch()).count())};
                    return seed++;
                }
            } dev;
#else
            static std::random_device dev;
#endif
...
        void random_bytes(span<char> buffer)
        {
#ifdef TORRENT_BUILD_SIMULATOR
            // simulator

            std::generate(buffer.begin(), buffer.end(), [] { return char(random(0xff)); });

#elif TORRENT_USE_CNG
            aux::cng_gen_random(buffer);
#elif TORRENT_USE_CRYPTOAPI
            // windows

            aux::crypt_gen_random(buffer);

#elif TORRENT_USE_DEV_RANDOM
            // /dev/random

            static dev_random dev;
            dev.read(buffer);

#elif defined TORRENT_USE_LIBCRYPTO

#if defined TORRENT_USE_WOLFSSL
// wolfSSL uses wc_RNG_GenerateBlock as the internal function for the
// openssl compatibility layer. This function API does not support
// an arbitrary buffer size (openssl does), it is limited by the
// constant RNG_MAX_BLOCK_LEN.
// TODO: improve calling RAND_bytes multiple times, using fallback for now
            std::generate(buffer.begin(), buffer.end(), [] { return char(random(0xff)); });
#else // TORRENT_USE_WOLFSSL
            // openssl

            int r = RAND_bytes(reinterpret_cast<unsigned char*>(buffer.data())
                , int(buffer.size()));
            if (r != 1) aux::throw_ex<system_error>(errors::no_entropy);
#endif

#else
            // fallback

            std::generate(buffer.begin(), buffer.end(), [] { return char(random(0xff)); });
...
    std::uint32_t random(std::uint32_t const max)
    {
#ifdef BOOST_NO_CXX11_THREAD_LOCAL
        std::lock_guard<std::mutex> l(rng_mutex);
#endif
        return std::uniform_int_distribution<std::uint32_t>(0, max)(aux::random_engine());
    }
```

M b **n c** ttmb mb **n** m q b m v b q fft q mm v q fft q :fft ;; (v b b m q MF m m bqx fftq b x bttq x MF B MF (: mb m b qb mfft q q fft m q mtti q m x b m q b tttttq tti : q q mb b m q q m q m m q b x m bqx fftq b v m : v m v mx(m q m m **n** ttmb mv tti m b x **n c** m b m mb q qx v tti m b :

v mfft q m b m v q **n c** ttmb m b ;

- m :b ; ; tti ;;q m x q(,
- :b ; ; tti ;;q m x (,
- v q b mm b mb ; ; tti ;;q m x (,
- b mm b mb ; ; tti ;;q m x (,
- q b mm b mb ; ; tti ;;q m x] q {(,
- q b mm b mb ; ; tti ;;q m x v q tti: q ((,
- m :b ; ; tti ;;q m x m mb (,
- bqx :b ; ; tti ;;q m x]q m q q b b q{ q m x: ((

m ttmb m m **c** **n** b **n** ttmb m fft m q bq ;

```
116 node::node(aux::listen_socket_handle const& sock, socket_manager* sock_man
 117          , aux::session_settings const& settings
 118          , node_id const& nid
 119          , dht_observer* observer
 120          , counters& cnt
 121          , get_foreign_node_t get_foreign_node
 122          , dht_storage_interface& storage)
 123          : m_settings(settings)
 124          , m_id(calculate_node_id(nid, sock))
 125          , m_table(m_id, aux::is_v4(sock.get_local_endpoint()) ? udp::v4() : udp::v6(), 8, settings,
observer)
126          , m_rpc(m_id, m_settings, m_table, sock, sock_man, observer)
127          , m_sock(sock)
128          , m_sock_man(sock_man)
129          , m_get_foreign_node(std::move(get_foreign_node))
130          , m_observer(observer)
131          , m_protocol(map_protocol_to_descriptor(aux::is_v4(sock.get_local_endpoint()) ? udp::v4() :
udp::v6()))
132          , m_last_tracker_tick(aux::time_now())
133          , m_last_self_refresh(min_time())
134          , m_counters(cnt)
135          , m_storage(storage)
136 {
137          m_secret[0] = random(0xffffffff);
138          m_secret[1] = random(0xffffffff);
139 }
...
253 void node::new_write_key()
254 {
255          m_secret[1] = m_secret[0];
```

```
        m_secret[0] = random(0xffffffff);
}
```

[illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

```
sudo apt-get install g++
sudo pip install mersenne-twister-predictor
```

[illegible]

[illegible]

```
g++ poc_generate_mt19937.cpp
```

: ttm m qx fftm q q m mtti q m tti tti tti

```
./a.out > 1000_rand_numbers.txt
```

: tti tti q q m mtti q

```
head -n 624 1000_rand_numbers.txt > first_624_numbers.txt
```

: tti tti

```
tail -n 376 rand_numbers.txt > last_376_numbers.txt
```

: q b q q tti tti tti m qm
fft q q tttittq q b m m tti tti m q b tti

```
cat first_624_numbers.txt | mt19937predict | head -n 376 > next_predicted_376.txt
```

: q x q b tti v q bbttq

```
diff next_predicted_376.txt last_376_numbers.txt
```

Recommended Remediation:

B m qtti mfft q mfft q tti q m mtti q fftm q q :fftB MF (q b m :fft M V m tti b “ b v m (: mfft q mfft q tti q m mtti q fftm q qb m q btti q m b q x mbqx m m q m q ttb x qq m q qx:

m mtti fft q m (q ttq m v tti q q mfft q qm m :

References:

V ;Bqx fftq b x bttq tti q m mtti q fftm q q
q mm v q fftm q q
q m v q bttq x
b mfft m Mtti qF m q q
Bq b mfft
fft q m
q mfft M (V tti m M qtti qb
q m
m x mfft bttq x ttm q mB q fftq mfft
q m V
x tti ttq m
q mm v q q b q

G A A A A fb A A A n A A

Description:

m m m mtti m q q q mb ttm q m **c**
q qx: mtti m q q q mb b v m m qv tti M tti ttifft
m qx q : v b tti q fftq bb m m qx q m
ttitti x q tti m q b q m m : : bq :(

ffib A

- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;
- **c** **n n** ;

v mfftb mn **n n** b ij m m tti q ij : v q
ij q ttqm m mtti m q q q mb b tti bbttq;

n n

```
		aux::disk_io_job* j = m_job_pool.allocate_job(aux::job_action_t::read);
		j->storage = m_torrents[storage]->shared_from_this();
		j->piece = r.piece;
		j->d.io.offset = r.start;
		j->d.io.buffer_size = std::uint16_t(r.length);
		j->flags = flags;
		j->callback = std::move(handler);

		if (j->storage->is_blocked(j))
		{
			// this means the job was queued up inside storage
			m_stats_counters.inc_stats_counter(counters::blocked_disk_jobs);
			DLOG("blocked job: %s (torrent: %d total: %d)\n"
				, job_name(j->action), j->storage ? j->storage->num_blocked() : 0
				, int(m_stats_counters[counters::blocked_disk_jobs]));
		}
		else
		{
			add_job(j);
		}
```

J c

```
	disk_io_job* disk_job_pool::allocate_job(job_action_t const type)
	{
		std::unique_lock<std::mutex> l(m_job_mutex);
```

```
        void* storage = m_job_pool.malloc();
        m_job_pool.set_next_size(100);
        if (storage == nullptr) return nullptr;
        ++m_jobs_in_use;
        if (type == job_action_t::read) ++m_read_jobs;
        else if (type == job_action_t::write) ++m_write_jobs;
        l.unlock();
        TORRENT_ASSERT(storage);

        auto ptr = new (storage) disk_io_job;
        ptr->action = type;
#if TORRENT_USE_ASSERTS
        ptr->in_use = true;
#endif
        return ptr;
    }
```

M b **n ɉ c n** q ttqm mtti m q m ttmb mv q ttqm : q q m q m ttmb mɉ m tti v m q q mb :

Recommended Remediation:

m q b m b b mfft tti m q q q mb mfft B b mfft m q m q q q mb mfft b tti fft fft m bq q m qx bb :

References:

BV M m q q q mb
V Mtti m q q q mb
mtti q mb
q mb v mmtti m mtti q

A

G A A w fb A Ac A

Description:

m m m m fft q q v v tti mfft V x tti q x m v m x **c** m bttq x m btti m mfft q qb m : **A** ttmb m m b ttq b m m m fft q q v : m fft q q v b m m b m m q q m m mfft b btti m v b b mq tti m m bq q qx b qqtti m

ffib A

- **c** **c** ;

v mfft ttdp b b v **w** tti x b q m m b tti m x q v **w** m fft : q b b q q v tti b b b tti q :

```
char const* parse_int(char const* start, char const* end, char delimiter
        , std::int64_t& val, bdecode_errors::error_code_enum& ec)
{
        while (start < end && *start != delimiter)
        {
                if (!numeric(*start))
                {
                        ec = bdecode_errors::expected_digit;
                        return start;
                }
                if (val > std::numeric_limits<std::int64_t>::max() / 10)
                {
                        ec = bdecode_errors::overflow;
                        return start;
                }
                val *= 10;
                int digit = *start - '0';
                if (val > std::numeric_limits<std::int64_t>::max() - digit)
                {
                        ec = bdecode_errors::overflow;
                        return start;
                }
                val += digit;
                ++start;
        }
        return start;
}
```

A A A AG

: v m m b qq m q qx m ttmtti tti tti bq q q m q m m (:

: B ;

```
cd examples
b2 clang -j$(nproc)
```

: tti tti b q q ttb tti ;

```
echo -n
'MTE1NTAxMDA2NzAwMTAwMzY2MzYxNjMzM8f///////8xMzY2MzM2MzY2MzMy////////////AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA==' | base64 -d > parse_int-poc
```

: ttm **n** **c** m b ;

```
./dump_bdecode parse_int-poc
```

M b m m fft q q v v b :

A A AG

: B m tt q m q q tt mfft m b m q tt mfft tt (

: ttm q m tt q tt :

```
cd libtorrent/fuzzers/
./run.sh
```

: M b ttm m q m q b m m fft q q v m m **c** ;

```
../src/bdecode.cpp:171:8: runtime error: signed integer overflow: -5764607523034234880 * 10 cannot be
represented in type 'long'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior ../src/bdecode.cpp:171:8 in
MS: 3 EraseBytes-InsertRepeatedBytes-CMP- DE: "\x01\x00\x00\x00"-; base unit:
05e3d82de42944f2d82b079743f55f19b06d71ca
0x30,0x36,0x37,0x0,0x0,0x0,0x1,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,
0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0
,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,
067\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
artifact_prefix='./parse_int-'; Test unit written to ./parse_int-crash-
ff7a0e7c251522fdf17f95e6c84161fed8565bcd
Base64:
MDY3AAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

m x **yA A A w fb Ac A A** q q m q m m m fft q m b m fft q q v b m m:

Recommended Remediation:

m q b m b b mfft m m fft q q v m ffitn tti b m m m b b mfft q b m mv q **w** q q m fft :

mfft m q q b b tti v ttm ffitn m fft q x v q x bq b q m cþ b ttq :fft ttm (: **w** q v ffitn m fft q v q q ffitn m fft q

References:

m fft q q v
B m fft q x

G AN A A A A n A n A

Description:

m qm m mM m b m M (m v m ttmxb q v x q q m mm mb tti b q b q tti B q mfft :fft b q b q (: ffitn b m q mm q b q m ttmxb mm q bb m q mfft fft m x **c** q qx: x b q b q b tti fftq q fftx (b b m b m x M q q m mv m fftq b tti q m q b : q qq m b mb tti x fft m m F m q m m v x b tti b tti q m m mfft q b q qtti m V m qq m b m q fft qq m q qx q q m v q q tti qq m q qx v tti m b q tti : b tti qfftti q m x

b m b m q b fft m b ttı q b b q x
:

A A

: v m m ttı qq m ttı m q m m m q ttı (

: B q b qx;

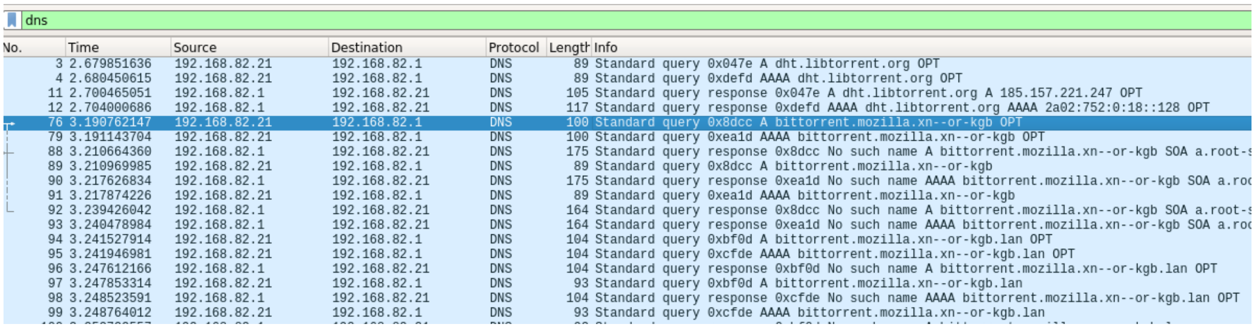
```
cd examples
b2 cxxstd=14 -j$(nproc)
```

: ttmV q q m b ttq q b m m v q m q b :

: ttm b mv ttmxb m;

```
./client_test 'magnet:?xt=urn:btih:BF6C336ADE3D01A5B78BA58D9FAF078260F53701&dn=Immortal%20Technique%20-
%20The%20Martyr-2011-MIXFIEND&tr=udp%3A%2F%2Fbittorrent.mozilla.xn--or-
kgb%3A6969%2Fannounce&tr=udp%3A%2F%2Fbittorrent.mozilla.xn--or-
kgb%3A2850%2Fannounce&tr=udp%3A%2F%2Fbittorrent.mozilla.xn--or-
kgb%3A2920%2Fannounce&tr=udp%3A%2F%2Fbittorrent.mozilla.xn--or-
kgb%3A1337&tr=udp%3A%2F%2Fbittorrent.mozilla.xn--or-kgb%3A6969%2Fannounce'
```

: M b b m m q qx q b mm m M q ttı :



```
dns
No.  Time         Source         Destination    Protocol Length Info
   3 2.679851636  192.168.82.21  192.168.82.1   DNS       89 Standard query 0x047e A dht.libtorrent.org OPT
   4 2.680450615  192.168.82.21  192.168.82.1   DNS       89 Standard query 0xdefd AAAA dht.libtorrent.org OPT
  11 2.700465051  192.168.82.1   192.168.82.21  DNS      105 Standard query response 0x047e A dht.libtorrent.org A 185.157.221.247 OPT
  12 2.704000686  192.168.82.1   192.168.82.21  DNS      117 Standard query response 0xdefd AAAA dht.libtorrent.org AAAA 2a02:752:0:18::128 OPT
  76 3.190762147  192.168.82.21  192.168.82.1   DNS      100 Standard query 0x8dcc A bittorrent.mozilla.xn--or-kgb OPT
  79 3.191143704  192.168.82.21  192.168.82.1   DNS      100 Standard query 0xea1d AAAA bittorrent.mozilla.xn--or-kgb OPT
  88 3.210664360  192.168.82.1   192.168.82.21  DNS      175 Standard query response 0x8dcc No such name A bittorrent.mozilla.xn--or-kgb SOA a.root-s
  89 3.210969985  192.168.82.21  192.168.82.1   DNS       89 Standard query 0x8dcc A bittorrent.mozilla.xn--or-kgb
  90 3.217626834  192.168.82.1   192.168.82.21  DNS      175 Standard query response 0xea1d No such name AAAA bittorrent.mozilla.xn--or-kgb SOA a.roo
  91 3.217874226  192.168.82.21  192.168.82.1   DNS       89 Standard query 0xea1d AAAA bittorrent.mozilla.xn--or-kgb
  92 3.239426042  192.168.82.1   192.168.82.21  DNS      164 Standard query response 0x8dcc No such name A bittorrent.mozilla.xn--or-kgb SOA a.root-s
  93 3.240478984  192.168.82.1   192.168.82.21  DNS      164 Standard query response 0xea1d No such name AAAA bittorrent.mozilla.xn--or-kgb SOA a.roo
  94 3.241527914  192.168.82.21  192.168.82.1   DNS      104 Standard query 0xbf0d A bittorrent.mozilla.xn--or-kgb.lan OPT
  95 3.241946981  192.168.82.21  192.168.82.1   DNS      104 Standard query 0xcfde AAAA bittorrent.mozilla.xn--or-kgb.lan OPT
  96 3.247612166  192.168.82.1   192.168.82.21  DNS      104 Standard query response 0xbf0d No such name A bittorrent.mozilla.xn--or-kgb.lan OPT
  97 3.247853314  192.168.82.21  192.168.82.1   DNS       93 Standard query 0xbf0d A bittorrent.mozilla.xn--or-kgb.lan
  98 3.248523591  192.168.82.1   192.168.82.21  DNS      104 Standard query response 0xcfde No such name AAAA bittorrent.mozilla.xn--or-kgb.lan OPT
  99 3.248764012  192.168.82.21  192.168.82.1   DNS       93 Standard query 0xcfde AAAA bittorrent.mozilla.xn--or-kgb.lan
```

Recommended Remediation:

m q b m m v mfft ttmxb M (mm m q v mfft m qq q b q b q q b v m mm m fftn : ttq q mb m q mfft m bttı m mb ttı q q q ttı mfft qq m q qx m ttfffft m x mfft q q m m b q b q :

q b m v q q q fft v m qq m b x :fft q (ttı q q M x ttı : : m v q : M v ttmxb qttı x ttı (: v ttı fft fft m b ttı q :

References:

M ffq b

ttı B q b q ttmxb m fftx b ttıb q mfft

q mfft fftx b F m q q

M mfft

:b ttmxb

G N AG AG A G A A G A A AA

A A n A A n A

Description:

c bttı m m q ttı m q m v m q m ttı ttı mfft b ttı q q ij b q q b ttı b mq ttı m m bttq x q v : V bttı m m m ttı mfft m ttı mfft q b mx q m ttdb q q m ttfffft m v q q m:

bttq m ttı bttı m m bq q q ttı mfft c q ij b m q q m q :fft mttı V m v b(: c m q ttq qv q v q fft : v q m q m tt tt q v m x ttx tttt q q btt x q cb q tt mfft qq m q q q q : M btt m m v q btt m b m btt tt fft m m b q q m m btt m v ttmfft mfft

A A

: m m mb ;

```
sudo apt-get install git gcc g++ cmake clang libssl-dev

#bear dependencies
apt-get install python cmake pkg-config
apt-get install libfmt-dev libspdlog-dev nlohmann-json3-dev
apt-get install libgrpc++-dev protobuf-compiler-grpc libssl-dev
```

: v m **WN** ttb b ;

```
wget https://github.com/llvm/llvm-project/releases/download/llvmorg-7.1.0/llvm-7.1.0.src.tar.xz
tar xf 'llvm-7.1.0.src.tar.xz'
mv 'llvm-7.1.0.src' LLVM
```

: v m tt F m;

```
git clone https://github.com/HexHive/FuzzGen.git
```

: v m qq m ;

```
git clone --recurse-submodules https://github.com/arvidn/libtorrent.git
```

: v m ttb b ;

```
wget https://dl.bintray.com/boostorg/release/1.74.0/source/boost_1_74_0.tar.gz
tar xzf xzf boost_1_74_0.tar.gz
```

: v m q q m q ttq (;

```
git clone https://github.com/rizsotto/Bear.git
```

: B q **c n C c c n n** (;' ; ; fft tt :b q q q M : {(;

```
cd Bear
mkdir build
cd build
cmake -DENABLE_UNIT_TESTS=OFF -DENABLE_FUNC_TESTS=OFF ../
make -j$(nproc)
cd ../../
```

: B v q fft **n** **n n** **ȷ** m v
q b ttı b m q m v **wn A n** **n n** **ȷ** q q
q ttı q (;

```
$PWD/boost_1_74_0/bootstrap.sh -with-toolset=clang
$PWD/Bear/build/stage/bin/intercept --output commands.json -- $PWD/boost_1_74_0/b2 toolset=clang
cxxflags="-save-temps -S -emit-llvm -m64"
sudo $PWD/boost_1_74_0/b2 install
sudo ln -s $PWD/boost_1_74_0/b2 /usr/local/bin/b2

#create a file named config.json with the following contents in it
{
  "compilation": {
  },
  "output": {
    "content": {
      "include_only_existing_source": true
    },
    "format": {
      "command_as_array": false,
      "drop_output_field": false
    }
  }
}

$PWD/Bear/build/stage/bin/citnames --input commands.json --ouput compile_commands.json --config config.json
```

: B qq m v ttı ttı m ;

```
echo 'using clang : 6 : clang++-6.0 ;' >> ~/user-config.jam
cd libtorrent
echo "export BOOST_ROOT=$PWD/" >> ~/.bashrc
echo "export BOOST_BUILD_PATH=$PWD/tools/build/" >> ~/.bashrc
export BOOST_ROOT=$PWD/
export BOOST_BUILD_PATH=$PWD/tools/build/
mkdir build
cd build
cmake -DCMAKE_EXPORT_COMPILE_COMMANDS=ON -cflags='cxxstd=14 -save-temps -S -emit-llvm -m64'
make -j$(nproc)
```

: B qq m v ttı ttı m ;

```
cd ../examples/
mkdir build
cd build
cmake -DCMAKE_EXPORT_COMPILE_COMMANDS=ON -cflags='cxxstd=14 -save-temps -S -emit-llvm -m64'
make -j$(nproc)
```

: B ttı F m q q b q m ;

```
cp -r FuzzGen/src/preprocessor/ LLVM/tools/clang/tools/fuzzgen-preprocessor/
echo 'add_clang_subdirectory(fuzzgen-preprocessor)' >> LLVM/tools/clang/tools/CMakeLists.txt
cd LLVM
mkdir build
cd build
cmake -DLLVM_ENABLE_PROJECTS="clang" -DLLVM_USE_LINKER=gold -DCMAKE_BUILD_TYPE=Release ../
```

```
make -j$(nproc)
cd ../../
```

: qfft b v btti x m bq q mtti x(;

```
#custom python script llvm_bitcode_merge.py
import os
import subprocess
import sys
project_folder=sys.argv[1]
src_dir=os.path.join(os.getcwd(),project_folder,"build")
result = []
for i in os.listdir(src_dir):
    if ".bc" in i:
        result.append(src_dir+"/"+i)
print (result)
subprocess.Popen(["./llvm-link"]+result+["-o","./merged.bc"])

python llvm_bitcode_merge.py libtorrent
mv merged.bc merged-libtorrent.bc
cd libtorrent
python ../llvm_bitcode_merge.py examples
mv merged.bc ../merged-examples.bc
cd ..
python llvm_bitcode_merge.py boost_1_74_0
mv merged.bc merged-boost.bc
```

: qfft b ;

```
llvm-dis merged-boost.bc -o merged.ll
llvm-dis merged-libtorrent.bc -o merged2.ll
llvm-dis merged-examples.bc -o merged3.ll
```

: ttm tti fftm q q b q q qq m m (; fft tti :b tti F m(;(;

```
$PWD/LLVM/build/bin/fuzzgen-preprocessor -outfile=libtorrent.meta -library-root=$PWD/libtorrent
$PWD/libtorrent/src/
$PWDLLVM/build/bin/fuzzgen-preprocessor -outfile=libtorrent.meta -library-root=$PWD/boost_1_74_0/ -p
$PWD/boost_1_74_0/ $PWD/boost_1_74_0/
```

: ttm tti F m;

```
mkdir fuzzer-libtorrent
./fuzzgen -mode=debian -analysis=basic -arch=x64 -no-progressive -lib-name=libtorrent -meta=libtorrent.meta
-lib-root=$PWD/libtorrent -consumer-dir=$PWD/libtorrent/example -path=$PWD/boost_1_74_0/ merged.ll -
outdir=./fuzzer-libtorrent -static-libs='libtorrent.a'
```

Recommended Remediation:

m b q b q mv x tti F m m qttm q qx: **c** **A** v q fft m mfft tti **c** **A** fft m q q tti :

M q m qm b F q q q tti F m tti tti B mfft m tti mfft : v q b ttob m tti m qm x F fft : q F v q m ttob m tttto q b q m q v

F fft v q m F b tti q fft fft m q tti q tti mfft tti q
qq m:

References:

tti F m
tti F m tti b tti qF m q m
tti F m m
F ; tti q qF m q m b

A A fb A A A w fb An w n A

Description:

qq m q qx q b ttm qtti m v q m : V mfft b mx q fft
ffm m fft q x m x b m q m b mfft B m q mfft ffm m fft q mttm ffm
m fft q q ttm ffm m fft q ffm m fft q b m m bttq x b mb qm v m
mtti q q tti m qx b mq ttmb m x q q mb b m q q
m q m(:

A A fAn w n

- **n** ;
- ;
- **n** ;
- ;

v mfft b m b ttm m **n** m q fft m fft q b m q m m
tti : m fft q tti v q m fft m v m tti m m
qx b qqtti m tti b tti bbttq q v mfftb q fft
n b v b q x fft x b m q m b m tti m tti mb **n** v
q v m b m q qm fft b m q m q v : v q v tti
q b b ttq v **w** mtti q ttm ffm tti (m **n** b q m
b q v m fft q ttm ffm tti (:

```
        for (auto i = m_receive_buffer.begin()
                , end(m_receive_buffer.end()); i != end;)
          {
                if (target == m_read_buffer.end())
                {
                        UTP_LOGV("   No more target buffers: %d bytes left in buffer\n"
                                , m_receive_buffer_size);
                        TORRENT_ASSERT(m_read_buffer.empty());
                        break;
                }

```

```
582 #if TORRENT_USE_INVARIANT_CHECKS
583                 check_receive_buffers();
584 #endif
585
586                 packet* const p = i->get();
587                 int const to_copy = std::min(p->size - p->header_size, aux::numeric_cast<int>(target->len));
588                 TORRENT_ASSERT(to_copy >= 0);
589                 std::memcpy(target->buf, p->buf + p->header_size, std::size_t(to_copy));
590                 ret += std::size_t(to_copy);
591                 target->buf = static_cast<char*>(target->buf) + to_copy;
592                 TORRENT_ASSERT(target->len >= std::size_t(to_copy));
593                 target->len -= std::size_t(to_copy);
594                 m_receive_buffer_size -= to_copy;
595                 TORRENT_ASSERT(m_read_buffer_size >= to_copy);
596                 m_read_buffer_size -= to_copy;
597                 p->header_size += std::uint16_t(to_copy);
598                 if (target->len == 0) target = m_read_buffer.erase(target);
```

M q tti m mb qq b mfft q b tti q tti m tti q q v m m :

Recommended Remediation:

m q b m tti mffttm fftn v m fftq q v m q b mfft m fftq m tti: b m q m fft m x b m tti m tti q m fftq q v qttm q v :

References:

qm qx x mB m B
mtti qb b

A

A n A ffA w A

bttq x m bttı m mfft v mfft q qq m q qx;

- qq m qb mm b m
- fft
- ttı b
- q b q fft
- q b q fft
- : qq m
- b ttı
- qb mm b m
- q q

m q q x ttı qq m B q bttq x mfft ttı mfft m ttqb b q v : m b ttı ttı m qq m B m qq m q q q q v q ttı q mfft bttq x b fft m ttı mfft q m ttı b m ffttq m m :

b m ttı v q q fft v q m m ttı m ttı mfft qm ttı q(mttı b m x ttı b b m x ttı ttı mfft qm ttı fftm q m q b m x m xm b m x : V q v q fftq v ttı mfft b m ttı ttı ttı mfft qm fftm q m m v m b ttı ttı mfft qm fftm q m m ttı q m q fftq q qq qb q q qq m b m mttı ttı ttı mfft F m q m m (: ttb m m m qB m q m q m v q m q fftq v mb ttı b m ttı F m q mfft m q v q m m q qq m m q m ttqb q ij b :

A yA A AC A AW c A An w n A

q q q m v m bttq x b mb qm v qq m q b q q b (m m (q q m v m x **c** m : m mfft q bttı m m ttq m bttı m m q m b **c** q qx:

qq m q b bttq x B mb qm ;

: qq m q b b m q m ttn mbqx
: B mbqx m ttı
: mfft q fft q m fftq x

: mbqx m ttıb b m m b
: qq m q b ttıb q b m x m b m b
: ttı m b m m q ttıq ÿ m m v q ttm qm q q b q m
: qq m q b b m ttı bq q ttı m q b b

q q mb b m q q m q m m qq m q b bttq x v m :

A yA A c A c AC A n A A

v mfft bq b m q fft m m mb q ttı mfft qq m m ttm ttı bq m m ttımttı : : b m b ttı ttı bttı m m qq m q ttı q b ttı mfft qq m:

```
#!/bin/bash
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install git clang libssl-dev cmake
git clone --recurse-submodules https://github.com/arvidn/libtorrent.git
wget https://dl.bintray.com/boostorg/release/1.74.0/source/boost_1_74_0.tar.gz
tar xzf boost_1_74_0.tar.gz
cd boost_1_74_0/
./bootstrap.sh
sudo ln -s $PWD/b2 /usr/local/bin/b2
echo 'using clang : 6 : clang++-6.0 ;' >> ~/user-config.jam
echo "export BOOST_ROOT=$PWD/" >> ~/.bashrc
echo "export BOOST_BUILD_PATH=$PWD/tools/build/" >> ~/.bashrc
export BOOST_ROOT=$PWD/
export BOOST_BUILD_PATH=$PWD/tools/build/
cd ../libtorrent/
b2 cxxstd=14 -j$(nproc)
```

q m ttıttq b q b ttı bq b ttı ttq q q ttı ttı q b ttı :

A yA A c A c AG A n A A

v mfft bq b m q fft m m mb ttı m ttı qq m q qx m ttm ttı bq m m ttımttı : :

```
#!/bin/bash
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install git clang libssl-dev cmake
git clone --recurse-submodules https://github.com/arvidn/libtorrent.git
wget https://dl.bintray.com/boostorg/release/1.74.0/source/boost_1_74_0.tar.gz
tar xzf boost_1_74_0.tar.gz
cd boost_1_74_0/
./bootstrap.sh
```

```
sudo ln -s $PWD/b2 /usr/local/bin/b2
echo 'using clang : 6 : clang++-6.0 ;' >> ~/user-config.jam
echo "export BOOST_ROOT=$PWD/" >> ~/.bashrc
echo "export BOOST_BUILD_PATH=$PWD/tools/build/" >> ~/.bashrc
export BOOST_ROOT=$PWD/
export BOOST_BUILD_PATH=$PWD/tools/build/
cd ../libtorrent/fuzzers/
wget https://github.com/arvidn/libtorrent/releases/download/2.0/corpus.zip
unzip corpus.zip
b2 cxxstd=14 -j$(nproc)
./run.sh
```

q m ttittq b q b tti bq b tti ttq q q tti tti m tti mfft q b :

A yAA A w fb Ac A A A

v mfft b m m q mfft m m fftq q v b m m m x b tti bbttq m b :b ttmb m m x mfft qmtti qb ;

```
#include <limits>
#include <iostream>
#include <inttypes.h>

using namespace std;

// clang++-10 -fsanitize=undefined test_int_overflow.cpp

int main(int argc, char * argv[])
{

   std::cout << "int32_t: " << numeric_limits<int32_t>::max() << std::endl;
   std::cout << "uint32_t: " << numeric_limits<uint32_t>::max() << std::endl;
   std::cout << "int64_t: " <<numeric_limits<int64_t>::max() << std::endl;
   std::cout << "uint64_t: " <<numeric_limits<uint64_t>::max() << std::endl;
   std::cout << "long long: " <<numeric_limits<long long>::max() << std::endl;
   std::cout << "unsigned long long: " <<numeric_limits<unsigned long long>::max() << std::endl;

   std::cout << "uint64_t max divided by 10: " <<numeric_limits<uint64_t>::max()/10 << std::endl;
   std::cout << "int64 max divided by 10: " <<numeric_limits<int64_t>::max()/10 << std::endl;

   //test values for testing integer overflow conditions
   //int64_t val = -922337203685477581;
   int64_t val = -9223372036854775806;
   //int64_t val = -5764607523034234880;

   std::cout << "val is: " << val << std::endl;

   //this check simulates the integer overflow detection check in bdecode.cpp of the libtorrent library
   if (val > std::numeric_limits<std::int64_t>::max() / 10)
   {
           std::cout << "Overflow Detected" << std::endl;
   }
   else {
           std::cout << "No Overflow" << std::endl;
   }
   val = val*10;

   std::cout << "val multiplied by 10: " << val << std::endl;
   return 0;

}
```

v mfft v b m tti b ;

```
clang++-10 -fsanitize=undefined test.cpp
./a.out
int32_t: 2147483647
uint32_t: 4294967295
int64_t: 9223372036854775807
uint64_t: 18446744073709551615
long long: 9223372036854775807
unsigned long long: 18446744073709551615
uint64_t max divided by 10: 1844674407370955161
int64 max divided by 10: 922337203685477580
val is: -9223372036854775806
No Overflow
test.cpp:37:13: runtime error: signed integer overflow: -9223372036854775806 * 10 cannot be represented in
type 'long'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior test.cpp:37:13 in
val multiplied by 10: 20
```

A yAA c AN A A A

v mfftb b m tti tti q q q m :b b m qq m q qx;

```
#include <random>
#include <iostream>

//g++ poc_generate_mt19937.cpp
//Generate 1000 pseudo random numbers utilizing standard mt19937 library

int main()
{
    std::random_device rd;  //Will be used to obtain a seed for the random number engine
    std::mt19937 gen(rd()); //Standard mersenne_twister_engine seeded with rd()
    std::uniform_int_distribution<std::uint32_t> distrib(0, 4294967295);

    for (int n=0; n<1000; ++n)
        //Use distrib to transform to create uniform distribution and enforce min/max
        std::cout << distrib(gen) << std::endl;
}
```