New issue

Jump to bottom

Certificate verification discrepancy between OpenSSL and mbed TLS #3629

Closed **guidovranken** opened this issue on Sep 1, 2020 · 6 comments

Assignees

Labels bug component-x509

guidovranken commented on Sep 1, 2020 Contributor

Description

- Type: Bug
- Priority: Unclear

A verification discrepancy found with differential fuzzing. OpenSSL fails to verify `discrepancy_cert` against the GlobalSign CA cert whereas mbed TLS succeeds. This might be worth looking into as it could indicate a (security) bug.

Bug

OS
linux

mbed TLS build:
Latest git checkout, default configuration.

Peer device TLS stack and version
Not applicable

Expected behavior
Verification fails

Actual behavior
Verification succeeds

Steps to reproduce

Compile and run:

```
#include <mbedtls/x509_crt.h>
#include <openssl/x509.h>

#define CF_CHECK_EQ(expr, res) if ( (expr) != (res) ) { goto end; }
#define CF_CHECK_NE(expr, res) if ( (expr) == (res) ) { goto end; }

const unsigned char globalsign[] = {
  0x30, 0x82, 0x03, 0xba, 0x30, 0x82, 0x02, 0xa2, 0xa0, 0x03, 0x02, 0x01,
  0x02, 0x02, 0x0b, 0x04, 0x00, 0x00, 0x00, 0x00, 0x01, 0x0f, 0x86, 0x26,
  0xe6, 0x0d, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86, 0x48, 0x86, 0xf7, 0x0d,
  0x01, 0x01, 0x05, 0x05, 0x00, 0x30, 0x4c, 0x31, 0x20, 0x30, 0x1e, 0x06,
  0x03, 0x55, 0x04, 0x0b, 0x13, 0x17, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c,
  0x53, 0x69, 0x67, 0x6e, 0x20, 0x52, 0x6f, 0x6f, 0x74, 0x20, 0x43, 0x41,
  0x20, 0x2d, 0x20, 0x52, 0x32, 0x31, 0x13, 0x30, 0x11, 0x06, 0x03, 0x55,
  0x04, 0x0a, 0x13, 0x0a, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x53, 0x69,
  0x67, 0x6e, 0x31, 0x13, 0x30, 0x11, 0x06, 0x03, 0x55, 0x04, 0x03, 0x13,
  0x0a, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x53, 0x69, 0x67, 0x6e, 0x30,
  0x1e, 0x17, 0x0d, 0x30, 0x36, 0x31, 0x32, 0x31, 0x35, 0x30, 0x38, 0x30,
  0x30, 0x30, 0x30, 0x5a, 0x17, 0x0d, 0x32, 0x31, 0x31, 0x32, 0x31, 0x35,
  0x30, 0x38, 0x30, 0x30, 0x30, 0x30, 0x5a, 0x30, 0x4c, 0x31, 0x20, 0x30,
  0x1e, 0x06, 0x03, 0x55, 0x04, 0x0b, 0x13, 0x17, 0x47, 0x6c, 0x6f, 0x62,
  0x61, 0x6c, 0x53, 0x69, 0x67, 0x6e, 0x20, 0x52, 0x6f, 0x6f, 0x74, 0x20,
  0x43, 0x41, 0x20, 0x2d, 0x20, 0x52, 0x32, 0x31, 0x13, 0x30, 0x11, 0x06,
  0x03, 0x55, 0x04, 0x0a, 0x13, 0x0a, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c,
  0x53, 0x69, 0x67, 0x6e, 0x31, 0x13, 0x30, 0x11, 0x06, 0x03, 0x55, 0x04,
  0x03, 0x13, 0x0a, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x53, 0x69, 0x67,
  0x6e, 0x30, 0x82, 0x01, 0x22, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86, 0x48,
  0x86, 0xf7, 0x0d, 0x01, 0x01, 0x01, 0x05, 0x00, 0x03, 0x82, 0x01, 0x0f,
  0x00, 0x30, 0x82, 0x01, 0x0a, 0x02, 0x82, 0x01, 0x01, 0x00, 0xa6, 0xcf,
  0x24, 0x0e, 0xbe, 0x2e, 0x6f, 0x28, 0x99, 0x45, 0x42, 0xc4, 0xab, 0x3e,
  0x21, 0x54, 0x9b, 0x0b, 0xd3, 0x7f, 0x84, 0x70, 0xfa, 0x12, 0xb3, 0xcb,
  0xbf, 0x87, 0x5f, 0xc6, 0x7f, 0x86, 0xd3, 0xb2, 0x30, 0x5c, 0xd6, 0xfd,
  0xad, 0xf1, 0x7b, 0xdc, 0xe5, 0xf8, 0x60, 0x96, 0x09, 0x92, 0x10, 0xf5,
  0xd0, 0x53, 0xde, 0xfb, 0x7b, 0x7e, 0x73, 0x88, 0xac, 0x52, 0x88, 0x7b,
  0x4a, 0xa6, 0xca, 0x49, 0xa6, 0x5e, 0xa8, 0xa7, 0x8c, 0x5a, 0x11, 0xbc,
  0x7a, 0x82, 0xeb, 0xbe, 0x8c, 0xe9, 0xb3, 0xac, 0x96, 0x25, 0x07, 0x97,
  0x4a, 0x99, 0x2a, 0x07, 0x2f, 0xb4, 0x1e, 0x77, 0xbf, 0x8a, 0x0f, 0xb5,
  0x02, 0x7c, 0x1b, 0x96, 0xb8, 0xc5, 0xb9, 0x3a, 0x2c, 0xbc, 0xd6, 0x12,
  0xb9, 0xeb, 0x59, 0x7d, 0xe2, 0xd0, 0x06, 0x86, 0x5f, 0x5e, 0x49, 0x6a,
  0xb5, 0x39, 0x5e, 0x88, 0x34, 0xec, 0xbc, 0x78, 0x0c, 0x08, 0x98, 0x84,
  0x6c, 0xa8, 0xcd, 0x4b, 0xb4, 0xa0, 0x7d, 0x0c, 0x79, 0x4d, 0xf0, 0xb8,
  0x2d, 0xcb, 0x21, 0xca, 0xd5, 0x6c, 0x5b, 0x7d, 0xe1, 0xa0, 0x29, 0x84,
  0xa1, 0xf9, 0xd3, 0x94, 0x49, 0xcb, 0x24, 0x62, 0x91, 0x20, 0xbc, 0xdd,
  0x0b, 0xd5, 0xd9, 0xcc, 0xf9, 0xea, 0x27, 0x0a, 0x2b, 0x73, 0x91, 0xc6,
  0x9d, 0x1b, 0xac, 0xc8, 0xcb, 0xe8, 0xe0, 0xa0, 0xf4, 0x2f, 0x90, 0x8b,
  0x4d, 0xfb, 0xb0, 0x36, 0x1b, 0xf6, 0x19, 0x7a, 0x85, 0xe0, 0x6d, 0xf2,
  0x61, 0x13, 0x88, 0x5c, 0x9f, 0xe0, 0x93, 0x0a, 0x51, 0x97, 0x8a, 0x5a,
  0xce, 0xaf, 0xab, 0xd5, 0xf7, 0xaa, 0x09, 0xaa, 0x60, 0xbd, 0xdc, 0xd9,
  0x5f, 0xdf, 0x72, 0xa9, 0x60, 0x13, 0x5e, 0x00, 0x01, 0xc9, 0x4a, 0xfa,
  0x3f, 0xa4, 0xea, 0x07, 0x03, 0x21, 0x02, 0x8e, 0x82, 0xca, 0x03, 0xc2,
  0x9b, 0x8f, 0x02, 0x03, 0x01, 0x00, 0x01, 0xa3, 0x81, 0x9c, 0x30, 0x81,
  0x99, 0x30, 0x0e, 0x06, 0x03, 0x55, 0x1d, 0x0f, 0x01, 0x01, 0xff, 0x04,
  0x04, 0x03, 0x02, 0x01, 0x06, 0x30, 0x0f, 0x06, 0x03, 0x55, 0x1d, 0x13,
  0x01, 0x01, 0xff, 0x04, 0x05, 0x30, 0x03, 0x01, 0x01, 0xff, 0x30, 0x1d,
  0x06, 0x03, 0x55, 0x1d, 0x0e, 0x04, 0x16, 0x04, 0x14, 0x9b, 0xe2, 0x07,
  0x57, 0x67, 0x1c, 0x1e, 0xc0, 0x6a, 0x06, 0xde, 0x59, 0xb4, 0x9a, 0x2d,
  0xdf, 0xdc, 0x19, 0x86, 0x2e, 0x30, 0x36, 0x06, 0x03, 0x55, 0x1d, 0x1f,
  0x04, 0x2f, 0x30, 0x2d, 0x30, 0x2b, 0xa0, 0x29, 0xa0, 0x27, 0x86, 0x25,
  0x68, 0x74, 0x74, 0x70, 0x3a, 0x2f, 0x2f, 0x63, 0x72, 0x6c, 0x2e, 0x67,
  0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x73, 0x69, 0x67, 0x6e, 0x2e, 0x6e, 0x65,
  0x74, 0x2f, 0x72, 0x6f, 0x6f, 0x74, 0x2d, 0x72, 0x32, 0x2e, 0x63, 0x72,
  0x6c, 0x30, 0x1f, 0x06, 0x03, 0x55, 0x1d, 0x23, 0x04, 0x18, 0x30, 0x16,
  0x80, 0x14, 0x9b, 0xe2, 0x07, 0x57, 0x67, 0x1c, 0x1e, 0xc0, 0x6a, 0x06,
  0xde, 0x59, 0xb4, 0x9a, 0x2d, 0xdf, 0xdc, 0x19, 0x86, 0x2e, 0x30, 0x0d,
  0x06, 0x09, 0x2a, 0x86, 0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01, 0x05, 0x05,
  0x00, 0x03, 0x82, 0x01, 0x01, 0x00, 0x99, 0x81, 0x53, 0x87, 0x1c, 0x68,
  0x97, 0x86, 0x91, 0xec, 0xe0, 0x4a, 0xb8, 0x44, 0x0b, 0xab, 0x81, 0xac,
  0x27, 0x4f, 0xd6, 0xc1, 0xb8, 0x1c, 0x43, 0x78, 0xb3, 0x0c, 0x9a, 0xfc,
  0xea, 0x2c, 0x3c, 0x6e, 0x61, 0x1b, 0x4d, 0x4b, 0x29, 0xf5, 0x9f, 0x05,
  0x1d, 0x26, 0xc1, 0xb8, 0xe9, 0x83, 0x00, 0x62, 0x45, 0xb6, 0xa9, 0x08,
  0x93, 0xb9, 0xa9, 0x33, 0x4b, 0x18, 0x9a, 0xc2, 0xf8, 0x87, 0x88, 0x4e,
  0xdb, 0xdd, 0x71, 0x34, 0x1a, 0xc1, 0x54, 0xda, 0x46, 0x3f, 0xe0, 0xd3,
  0x2a, 0xab, 0x6d, 0x54, 0x22, 0xf5, 0x3a, 0x62, 0xcd, 0x20, 0x6f, 0xba,
  0x29, 0x89, 0xd7, 0xdd, 0x91, 0xee, 0xd3, 0x5c, 0xa2, 0x3e, 0xa1, 0x5b,
  0x41, 0xf5, 0xdf, 0xe5, 0x64, 0x43, 0x2d, 0xe9, 0xd5, 0x39, 0xab, 0xd2,
  0xa2, 0xdf, 0xb7, 0x8b, 0xd0, 0xc0, 0x80, 0x19, 0x1c, 0x45, 0xc0, 0x2d,
  0x8c, 0xe8, 0xf8, 0x2d, 0xa4, 0x74, 0x56, 0x49, 0xc5, 0x05, 0xb5, 0x4f,
  0x15, 0xde, 0x6e, 0x44, 0x78, 0x39, 0x87, 0xa8, 0x7e, 0xbb, 0xf3, 0x79,
  0x18, 0x91, 0xbb, 0xf4, 0x6f, 0x9d, 0xc1, 0xf0, 0x8c, 0x35, 0x8c, 0x5d,
  0x01, 0xfb, 0xc3, 0x6d, 0xb9, 0xef, 0x44, 0x6d, 0x79, 0x46, 0x31, 0x7e,
  0x0a, 0xfe, 0xa9, 0x82, 0xc1, 0xff, 0xef, 0xab, 0x6e, 0x20, 0xc4, 0x50,
  0xc9, 0x5f, 0x9d, 0x4d, 0x9b, 0x17, 0x8c, 0x0c, 0xe5, 0x01, 0xc9, 0xa0,
  0x41, 0x6a, 0x73, 0x53, 0xfa, 0xa5, 0x50, 0xb4, 0x6e, 0x25, 0x0f, 0xfb,
  0x4c, 0x18, 0xf4, 0xfd, 0x52, 0xd9, 0x8e, 0x69, 0xb1, 0xe8, 0x11, 0x0f,
  0xde, 0x88, 0xd8, 0xfb, 0x1d, 0x49, 0xf7, 0xaa, 0xde, 0x95, 0xcf, 0x20,
  0x78, 0xc2, 0x60, 0x12, 0xdb, 0x25, 0x40, 0x8c, 0x6a, 0xfc, 0x7e, 0x42,
  0x38, 0x40, 0x64, 0x12, 0xf7, 0x9e, 0x81, 0xe1, 0x93, 0x2e
};

const unsigned char discrepancy_cert[] = {
 0x30, 0x82, 0x04, 0x4a, 0x30, 0x82, 0x03, 0x32, 0xa0, 0x03, 0x02, 0x01, 0x02, 0x02, 0x0d, 0x01,
 0xe3, 0xb4, 0x9a, 0xa1, 0x8d, 0x8a, 0xa9, 0x81, 0x25, 0x69, 0x50, 0xb8, 0x30, 0x0d, 0x06, 0x09,
 0x2a, 0x86, 0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01, 0x0b, 0x05, 0x00, 0x30, 0x4c, 0x31, 0x20, 0x30,
 0x1e, 0x06, 0x03, 0x55, 0x04, 0x0b, 0x13, 0x17, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x53, 0x69,
 0x67, 0x6e, 0x20, 0x52, 0x6f, 0x6f, 0x74, 0x20, 0x43, 0x41, 0x20, 0x2d, 0x20, 0x52, 0x32, 0x31,
 0x13, 0x30, 0x11, 0x06, 0x03, 0x55, 0x04, 0x0a, 0x13, 0x0a, 0x47, 0x6c, 0x6f, 0x62, 0x61, 0x6c,
 0x53, 0x69, 0x67, 0x6e, 0x31, 0x13, 0x30, 0x11, 0x06, 0x03, 0x55, 0x04, 0x03, 0x13, 0x0a, 0x47,
 0x6c, 0x6f, 0x62, 0x61, 0x6c, 0x53, 0x69, 0x67, 0x6e, 0x30, 0x1e, 0x17, 0x0d, 0x31, 0x37, 0x30,
 0x36, 0x31, 0x35, 0x30, 0x30, 0x30, 0x30, 0x34, 0x32, 0x5a, 0x17, 0x0d, 0x32, 0x31, 0x31, 0x32,
 0x31, 0x35, 0x30, 0x30, 0x30, 0x30, 0x34, 0x32, 0x5a, 0x30, 0x42, 0x31, 0x0b, 0x30, 0x09, 0x06,
 0x03, 0x55, 0x04, 0x06, 0x13, 0x02, 0x55, 0x53, 0x31, 0x1e, 0x30, 0x1c, 0x06, 0x03, 0x55, 0x04,
 0x0a, 0x13, 0x15, 0x47, 0x6f, 0x6f, 0x67, 0x6c, 0x65, 0x20, 0x54, 0x72, 0x75, 0x73, 0x74, 0x20,
 0x53, 0x65, 0x72, 0x76, 0x69, 0x63, 0x65, 0x73, 0x31, 0x13, 0x30, 0x11, 0x06, 0x03, 0x55, 0x04,
 0x03, 0x13, 0x0a, 0x47, 0x54, 0x53, 0x20, 0x43, 0x41, 0x20, 0x31, 0x4f, 0x31, 0x30, 0x82, 0x01,
 0x22, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86, 0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01, 0x01, 0x05, 0x00,
 0x03, 0x82, 0x01, 0x0f, 0x00, 0x30, 0x82, 0x01, 0x0a, 0x02, 0x82, 0x01, 0x01, 0x00, 0xd0, 0x18,
 0xcf, 0x45, 0xd4, 0x8b, 0xcd, 0xd3, 0x9c, 0xe4, 0x40, 0xef, 0x7e, 0xb4, 0xdd, 0x69, 0x21, 0x1b,
 0xc9, 0xcf, 0x3c, 0x8e, 0x4c, 0x75, 0xb9, 0x0f, 0x31, 0x19, 0x84, 0x3d, 0x9e, 0x3c, 0x29, 0xef,
 0x50, 0x0d, 0x10, 0x93, 0x6f, 0x05, 0x80, 0x80, 0x9f, 0x2a, 0xa0, 0xbd, 0x12, 0x4b, 0x02, 0xe1,
 0x3d, 0x9f, 0x58, 0x16, 0x24, 0xfe, 0x30, 0x9f, 0x0b, 0x74, 0x77, 0x55, 0x93, 0x1d, 0x4b, 0xf7,
 0x4d, 0xe1, 0x92, 0x82, 0x10, 0xf6, 0x51, 0xac, 0x0c, 0xc3, 0xb2, 0x22, 0x94, 0x0f, 0x34, 0x6b,
 0x98, 0x10, 0x49, 0xe7, 0x0b, 0x9d, 0x83, 0x39, 0xdd, 0x20, 0xc6, 0x1c, 0x2d, 0xef, 0xd1, 0x18,
 0x61, 0x65, 0xe7, 0x23, 0x83, 0x20, 0xa8, 0x23, 0x12, 0xff, 0xd2, 0x24, 0x7f, 0xd4, 0x2f, 0xe7,
 0x44, 0x6a, 0x5b, 0x4d, 0xd7, 0x50, 0x66, 0xb0, 0xaf, 0x9e, 0x42, 0x63, 0x05, 0xfb, 0xe0, 0x1c,
 0xc4, 0x63, 0x61, 0xaf, 0x9f, 0x6a, 0x33, 0xff, 0x62, 0x97, 0xbd, 0x48, 0xd9, 0xd3, 0x7c, 0x14,
 0x67, 0xdc, 0x75, 0xdc, 0x2e, 0x69, 0xe8, 0xf8, 0x6d, 0x78, 0x69, 0xd0, 0xb7, 0x10, 0x05, 0xb8,
 0xf1, 0x31, 0xc2, 0x3b, 0x24, 0xfd, 0x1a, 0x33, 0x74, 0xf8, 0x23, 0xe0, 0xec, 0x6b, 0x19, 0x8a,
 0x16, 0xc6, 0xe3, 0xcd, 0xa4, 0xcd, 0x0b, 0xdb, 0xb3, 0xa4, 0x59, 0x60, 0x38, 0x88, 0x3b, 0xad,
 0x1d, 0xb9, 0xc6, 0x8c, 0xa7, 0x53, 0x1b, 0xfc, 0xbc, 0xd9, 0xa4, 0xab, 0xbc, 0xdd, 0x3c, 0x61,
 0xd7, 0x93, 0x15, 0x98, 0xee, 0x81, 0xbd, 0x8f, 0xe2, 0x64, 0x47, 0x20, 0x40, 0x06, 0x4e, 0xd7,
 0xac, 0x97, 0xe8, 0xb9, 0xc0, 0x59, 0x12, 0xa1, 0x49, 0x25, 0x23, 0xe4, 0xed, 0x70, 0x34, 0x2c,
 0xa5, 0xb4, 0x63, 0x7c, 0xf9, 0xa3, 0x3d, 0x83, 0xd1, 0xcd, 0x6d, 0x24, 0xac, 0x07, 0x02, 0x03,
 0x01, 0x00, 0x01, 0xa3, 0x82, 0x01, 0x33, 0x30, 0x82, 0x01, 0x2f, 0x30, 0x0e, 0x06, 0x03, 0x55,
 0x1d, 0x0f, 0x01, 0x01, 0xff, 0x04, 0x04, 0x03, 0x02, 0x01, 0x86, 0x30, 0x1d, 0x06, 0x03, 0x55,
 0x1d, 0x25, 0x04, 0x16, 0x30, 0x14, 0x06, 0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x03, 0x01,
 0x06, 0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x03, 0x02, 0x30, 0x12, 0x06, 0x03, 0x55, 0x1d,
 0x13, 0x01, 0x01, 0xff, 0x04, 0x08, 0x30, 0x06, 0x01, 0x01, 0xff, 0x02, 0x01, 0x00, 0x30, 0x1d,
 0x06, 0x03, 0x55, 0x1d, 0x0e, 0x04, 0x16, 0x04, 0x14, 0x98, 0xd1, 0xf8, 0x6e, 0x10, 0xeb, 0xcf,
 0x9b, 0xec, 0x60, 0x9f, 0x18, 0x90, 0x1b, 0xa0, 0xeb, 0x7d, 0x09, 0xfd, 0x2b, 0x30, 0x1f, 0x06,
 0x03, 0x55, 0x1d, 0x23, 0x04, 0x18, 0x30, 0x16, 0x80, 0x14, 0x9b, 0xe2, 0x07, 0x57, 0x67, 0x1c,
 0x1e, 0xc0, 0x6a, 0x06, 0xde, 0x59, 0xb4, 0x9a, 0x2d, 0xdf, 0xdc, 0x19, 0x86, 0x2e, 0x30, 0x35,
 0x06, 0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x01, 0x01, 0x04, 0x29, 0x30, 0x27, 0x30, 0x25,
 0x06, 0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x30, 0x01, 0x86, 0x19, 0x68, 0x74, 0x74, 0x70,
 0x3a, 0x2f, 0x2f, 0x6f, 0x63, 0x73, 0x70, 0x2e, 0x70, 0x6b, 0x69, 0x2e, 0x67, 0x6f, 0x6f, 0x67,
 0x2f, 0x67, 0x73, 0x72, 0x32, 0x30, 0x32, 0x06, 0x03, 0x55, 0x1d, 0x1f, 0x04, 0x2b, 0x30, 0x29,
 0x30, 0x27, 0xa0, 0x25, 0xa0, 0x23, 0x86, 0x21, 0x68, 0x74, 0x74, 0x70, 0x3a, 0x2f, 0x2f, 0x63,
 0x72, 0x6c, 0x2e, 0x70, 0x6b, 0x69, 0x2e, 0x67, 0x6f, 0x6f, 0x67, 0x2f, 0x67, 0x73, 0x72, 0x32,
 0x2f, 0x67, 0x73, 0x72, 0x32, 0x2e, 0x63, 0x72, 0x6c, 0x30, 0x3f, 0x06, 0x03, 0x55, 0x1d, 0x20,
 0x04, 0x38, 0x30, 0x36, 0x30, 0x34, 0x06, 0x06, 0x67, 0x81, 0x0c, 0x01, 0x02, 0x02, 0x30, 0x2a,
 0x30, 0x28, 0x06, 0x08, 0x2b, 0x06, 0x01, 0x05, 0x05, 0x07, 0x02, 0x01, 0x16, 0x1c, 0x68, 0x74,
 0x74, 0x70, 0x73, 0x3a, 0x2f, 0x2f, 0x70, 0x6b, 0x69, 0x2e, 0x67, 0x6f, 0x6f, 0x67, 0x2f, 0x72,
 0x65, 0x70, 0x6f, 0x73, 0x69, 0x74, 0x6f, 0x72, 0x79, 0x2f, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86,
 0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01, 0x0b, 0x09, 0x00, 0x03, 0x82, 0x01, 0x01, 0x00, 0x1a, 0x80,
 0x3e, 0x36, 0x79, 0xfb, 0xf3, 0x2e, 0xa9, 0x46, 0x37, 0x7d, 0x5e, 0x54, 0x16, 0x35, 0xae, 0xc7,
 0x4e, 0x08, 0x99, 0xfe, 0xbd, 0xd1, 0x34, 0x69, 0x26, 0x52, 0x66, 0x07, 0x3d, 0x0a, 0xba, 0x49,
 0xcb, 0x62, 0xf4, 0xf1, 0x1a, 0x8e, 0xfc, 0x11, 0x4f, 0x68, 0x96, 0x4c, 0x74, 0x2b, 0xd3, 0x67,
 0xde, 0xb2, 0xa3, 0xaa, 0x05, 0x8d, 0x84, 0x4d, 0x4c, 0x20, 0x65, 0x0f, 0xa5, 0x96, 0xda, 0x0d,
 0x16, 0xf8, 0x6c, 0x3b, 0xdb, 0x6f, 0x04, 0x23, 0x88, 0x6b, 0x3a, 0x6c, 0xc1, 0x60, 0xbd, 0x68,
 0x9f, 0x71, 0x8e, 0xee, 0x2d, 0x58, 0x34, 0x07, 0xf0, 0xd5, 0x54, 0xe9, 0x86, 0x59, 0xfd, 0x7b,
 0x5e, 0x0d, 0x21, 0x94, 0xf5, 0x8c, 0xc9, 0xa8, 0xf8, 0xd8, 0xf2, 0xad, 0xcc, 0x0f, 0x1a, 0xf3,
 0x9a, 0xa7, 0xa9, 0x04, 0x27, 0xf9, 0xa3, 0xc9, 0xb0, 0xff, 0x02, 0x78, 0x6b, 0x61, 0xba, 0xc7,
 0x35, 0x2b, 0xe8, 0x56, 0xfa, 0x4f, 0xc3, 0x1c, 0x0c, 0xed, 0xb6, 0x3c, 0xb4, 0x4b, 0xea, 0xed,
 0xcc, 0xe1, 0x3c, 0xec, 0xdc, 0x0d, 0x8c, 0xd6, 0x3e, 0x9b, 0xca, 0x42, 0x58, 0x8b, 0xcc, 0x16,
 0x21, 0x17, 0x40, 0xbc, 0xa2, 0xd6, 0x66, 0xef, 0xda, 0xc4, 0x15, 0x5b, 0xcd, 0x89, 0xaa, 0x9b,
 0x09, 0x26, 0xe7, 0x32, 0xd2, 0x0d, 0x6e, 0x67, 0x20, 0x02, 0x5b, 0x10, 0xb0, 0x90, 0x09, 0x9c,
 0x0c, 0x1f, 0x9e, 0xad, 0xd8, 0x3b, 0xea, 0xa1, 0xfc, 0x6c, 0xe8, 0x10, 0x5c, 0x08, 0x52, 0x19,
 0x51, 0x2a, 0x71, 0xbb, 0xac, 0x7a, 0xb5, 0xdd, 0x15, 0xed, 0x2b, 0xc9, 0x08, 0x2a, 0x2c, 0x8a,
 0xb4, 0xa6, 0x21, 0xab, 0x63, 0xff, 0xd7, 0x52, 0x49, 0x50, 0xd0, 0x89, 0xb7, 0xad, 0xf2, 0xaf,
 0xfb, 0x50, 0xae, 0x2f, 0xe1, 0x95, 0x0d, 0xf3, 0x46, 0xad, 0x9d, 0x9c, 0xf5, 0xca, 0x27, 0xa4,
 0xeb, 0x4d, 0xb7, 0x8b, 0xd0, 0x77, 0x84, 0xc8, 0xc0, 0xea, 0x42, 0x21, 0x3a, 0x6f, 0x02, 0x1f,
 0x28, 0xbc, 0x22, 0x6a, 0xfd, 0xe0, 0x52, 0x58, 0xb5, 0xc8, 0x47, 0xb9, 0x1c, 0xc8, 0xb6, 0x0a,
 0x3b, 0xa7, 0x4d, 0x89, 0x5e, 0xea, 0xad, 0x95, 0x8e, 0x6a, 0x12, 0x87, 0x5b, 0xce, 0x95, 0x2e,
 0xd3, 0x26, 0x11, 0xa6, 0xbe, 0xa0, 0x20, 0xac, 0x32, 0x02, 0x8b, 0x20, 0xeb, 0x83, 0x1b, 0x2c,
 0xfd, 0x52, 0xa2, 0xb4, 0x44, 0xee, 0x52, 0x45, 0x2a, 0x2f, 0x5b, 0xbe, 0x15, 0xce, 0x78, 0xba,
 0x47, 0x19, 0x97, 0x98, 0xa9, 0x56, 0x23, 0xa9, 0x9f, 0x57, 0xe2, 0xd7, 0x92, 0xf6, 0x4c, 0x53,
 0x2f, 0x91, 0x2a, 0x91, 0xf2, 0x29, 0xf3, 0x4c, 0xf5, 0x5c, 0x1a, 0x80, 0xf7, 0x44, 0xd6, 0xb5,
 0x95, 0xb9, 0x36, 0x81, 0x56, 0x5f, 0x2c, 0xad, 0x96, 0xde, 0xbc, 0x73, 0x25, 0xe9, 0x3a, 0x46,
 0x91, 0x27, 0xa4, 0x1f, 0x4d, 0xb7, 0x8b, 0xd0, 0x77, 0x84, 0xc8, 0xc0, 0xea, 0x42, 0x21, 0x3a,
 0x6f, 0x02, 0x1f, 0x28, 0xbc, 0x22, 0x6a, 0xfd, 0xe0, 0x52, 0x58, 0xb5, 0xc8, 0x47, 0xb9, 0x1c,
 0xc8, 0xb6, 0x0a, 0x3b, 0xa7, 0x4d, 0x89, 0x5e, 0xea, 0xad, 0x95, 0x8e, 0x6a, 0x12, 0x87, 0x5b,
 0xce, 0x95, 0x2e, 0xd3, 0x26, 0x11, 0xa6, 0xbe, 0xa0, 0x20, 0xac, 0x32, 0x02, 0x8b, 0x20, 0xeb,
 0x83, 0x1b, 0x2c, 0xfd, 0x52, 0xa2, 0xb4, 0x44, 0xee, 0x52, 0x45, 0x2a, 0x2f, 0x5b, 0xbe, 0x15,
 0xce, 0x78, 0xba, 0x47, 0x19, 0x97, 0x98, 0xa9, 0x56, 0x23, 0xa9, 0x9f, 0x57, 0xe2, 0xd7, 0x92,
 0xf6, 0x4c, 0x53, 0x2f, 0x91, 0x2a, 0x91, 0xf2, 0x29, 0xf3, 0x4c, 0xf5, 0x5c, 0x1a, 0x80, 0xf7,
 0x44, 0xd6, 0xb5, 0x95, 0xb9, 0x36, 0x81, 0x56, 0x5f, 0x2c, 0xad, 0x96, 0x86, 0x48, 0xce, 0x3d,
 0x02, 0x60, 0x39, 0x0d, 0xfa, 0x32, 0x30, 0x32, 0x00, 0x00, 0x01, 0x71, 0x2b, 0x0e, 0x2a, 0x32,
 0xc9, 0xcc, 0x1a, 0xca, 0xe1, 0x00, 0x00, 0x00, 0x04, 0x03, 0x00, 0x00, 0x89, 0x00, 0x00, 0x00,
 0x01, 0xd0, 0x00, 0x00, 0x01, 0x04, 0x00, 0x00, 0x30, 0x80, 0x30, 0x80, 0x02, 0x02, 0x73, 0x32,
 0x30, 0x80, 0x06, 0x02, 0x30, 0x30, 0x00, 0x00, 0x30, 0x00, 0x30, 0x1e, 0x17, 0x0d, 0x31, 0x30,
 0x31, 0x31, 0x30, 0x30, 0x80, 0x30, 0x80, 0x02, 0x01, 0x28, 0x30, 0x03, 0x06, 0x01, 0x27, 0x30,
 0x00, 0x30, 0x80, 0x30, 0x80, 0x02, 0x01, 0xff, 0x30, 0x03, 0x06, 0x01, 0x2a, 0x30, 0x00, 0x30,
 0x80, 0x18, 0x00, 0x18, 0x00, 0x00, 0x00, 0x30, 0x00, 0x30, 0x2a, 0x86, 0x48, 0xce, 0x01, 0x01,
 0x3d, 0x48, 0xce, 0x3d, 0x02, 0x01, 0x06, 0x05, 0x67, 0x2b, 0x01, 0x04, 0x08, 0x00, 0x00, 0x03,
 0x10, 0x00, 0x02, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xdf, 0x40, 0x00, 0x00, 0x00, 0x00, 0x00,
 0xff, 0x04, 0x0c, 0x03, 0x09, 0x00, 0x00, 0x00, 0x00, 0x00, 0x06, 0x00, 0x01, 0x00, 0x00, 0x00,
 0x00, 0x30, 0x80, 0x06, 0x09, 0x60, 0x86, 0x48, 0x01, 0x86, 0xf8, 0x42, 0x01, 0x01, 0x04, 0x0c};

static void mbedtls(void) {
    mbedtls_x509_crt cert;
    mbedtls_x509_crt ca;

    /* noret */ mbedtls_x509_crt_init(&cert);
    /* noret */ mbedtls_x509_crt_init(&ca);

    CF_CHECK_EQ(mbedtls_x509_crt_parse(&cert, discrepancy_cert, sizeof(discrepancy_cert)), 0);
    CF_CHECK_EQ(mbedtls_x509_crt_parse(&ca, globalsign, sizeof(globalsign)), 0);

    {
        uint32_t flags;
        printf("mbed TLS:\n");
        if ( mbedtls_x509_crt_verify(&cert, &ca, NULL, NULL, &flags, NULL, NULL) == 0 ) {
            printf("Verification succeeded\n");
        } else {
            printf("Verification failed\n");
        }
    }

end:
    /* noret */ mbedtls_x509_crt_free(&cert);
    /* noret */ mbedtls_x509_crt_free(&ca);
}

static void openssl(void) {
    X509* x509 = NULL;
    X509* ca = NULL;
    X509_STORE* store = NULL;
    X509_STORE_CTX* storeCtx = NULL;

    {
        const unsigned char* p = discrepancy_cert;
        CF_CHECK_NE(d2i_X509(&x509, &p, sizeof(discrepancy_cert)), NULL);
    }

    {
        const unsigned char* p = globalsign;
        CF_CHECK_NE(d2i_X509(&ca, &p, sizeof(globalsign)), NULL);
    }

    CF_CHECK_NE(store = X509_STORE_new(), NULL);
    CF_CHECK_EQ(X509_STORE_add_cert(store, ca), 1);

    CF_CHECK_NE(storeCtx = X509_STORE_CTX_new(), NULL);
    CF_CHECK_EQ(X509_STORE_CTX_init(storeCtx, store, x509, NULL), 1);
    /* noret */ X509_STORE_CTX_set_flags(storeCtx, X509_V_FLAG_CB_ISSUER_CHECK);

    printf("OpenSSL:\n");
    if ( X509_verify_cert(storeCtx) == 1 ) {
        printf("Verification succeeded\n");
    } else {
        printf("Verification failed\n");
    }

end:
    X509_free(x509);
    X509_free(ca);
    X509_STORE_CTX_free(storeCtx);
    X509_STORE_free(store);
}

int main(void)
{
    mbedtls();
    openssl();
    return 0;
}
```

daverodgman assigned **paul-elliott-arm** on Sep 3, 2020

daverodgman added bug **component-x509** labels on Sep 7, 2020

paul-elliott-arm added this to **To Do** in **OBSOLETE - PLEASE SEE https://github.com/orgs/Mbed-TLS/projects/2** via automation on Oct 16, 2020

paul-elliott-arm moved this from **To Do** to **In Progress** in **OBSOLETE - PLEASE SEE https://github.com/orgs/Mbed-TLS/projects/2** on Oct 26, 2020

paul-elliott-arm commented on Nov 19, 2020 Contributor

Hi! Just as a question, do you know how this certificate was generated?

guidovranken commented on Nov 19, 2020 Contributor Author

Generated by a fuzzer. I probably used the OpenSSL OSS-Fuzz X509 corpus as a seed corpus, and it was mutated from that.

paul-elliott-arm commented on Nov 19, 2020 Contributor

Interesting, thank you.

guidovranken commented on Nov 20, 2020 Contributor Author

@paul-elliott-arm Can you contact me at guido@guidovranken.com? Thanks.

chris-jones-arm commented on Dec 17, 2020 Contributor

@paul-elliott-arm **@guidovranken** Can this issue be closed now as it appears to have been fixed in `ca17ebf` ?

paul-elliott-arm commented on Dec 17, 2020 Contributor

Yes, this only closed the internal issue. Closing this now.

paul-elliott-arm closed this as completed on Dec 17, 2020

OBSOLETE - PLEASE SEE https://github.com/orgs/Mbed-TLS/projects/2 automation moved this from **In Progress** to **Done** on Dec 17, 2020

bensze01 removed this from **Done** in **OBSOLETE - PLEASE SEE https://github.com/orgs/Mbed-TLS/projects/2** on Jan 13, 2021

Assignees

paul-elliott-arm

Labels

bug component-x509

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants