

DCMTK - Bug #740

Vulnerability in certificate verification code in dcmsign

2017-03-24 09:49 - Marco Eichelberg

|                   |                  |                 |            |
|-------------------|------------------|-----------------|------------|
| Status:           | Closed           | Start date:     | 2017-03-24 |
| Priority:         | High             | Due date:       |            |
| Assignee:         | Marco Eichelberg | % Done:         | 100%       |
| Category:         |                  | Estimated time: | 0:00 hour  |
| Target version:   | 3.6.2            | Compiler:       |            |
| Module:           | dcmsign          |                 |            |
| Operating System: |                  |                 |            |

**Description**

███ <[rlq1969612634@gmail.com](mailto:rlq1969612634@gmail.com)> writes:

Recently We made a large scale security static analysis on several open source projects, and found some mistakes in dcmthk-3.6.0. In dcmsign/libsrc/sicertvf.cc:122:

```
OFCondition SiCertificateVerifier::verifyCertificate(SiCertificate& certificate)
{
    errorCode = 0;
    X509 *rawcert = certificate.getRawCertificate();
    if (rawcert == NULL) return SI_EC_VerificationFailed_NoCertificate;
    X509_STORE_CTX ctx;
    X509_STORE_CTX_init(&ctx, x509store, rawcert, NULL);
    int ok = X509_verify_cert(&ctx); /* returns nonzero if successful */
    errorCode = X509_STORE_CTX_get_error(&ctx);
    X509_STORE_CTX_cleanup(&ctx);
    if (ok) return EC_Normal; else return SI_EC_VerificationFailed_NoTrust;
}
```

X509\_verify\_cert is a function which discover and verify X509 certicfte chain. If a complete chain can be built and validated this function returns 1, otherwise it return 0, in exceptional circumstances it can return -1. Here developers take wrong verification mode(ignore -1), the control expression (if (ok)) is true as in the case when -1 is returned. As a result, the program would behave as if the verification is valid, MITM attacks will occur .

The solution is turn the judgment statement if(ok) into if(ok==1).

History

#1 - 2017-03-24 16:54 - Marco Eichelberg

- Status changed from New to Closed
- Assignee set to Marco Eichelberg
- % Done changed from 0 to 100

Fixed by commit 3428613.