rules.sonarsource.com

Kotlin static code analysis: Server certificates should be verified during SSL/TLS connections

3 minutes

Validation of X.509 certificates is essential to create secure SSL/TLS sessions not vulnerable to man-in-the-middle attacks.

The certificate chain validation includes these steps:

- The certificate is issued by its parent Certificate Authority or the root CA trusted by the system.
- Each CA is allowed to issue certificates.
- Each certificate in the chain is not expired.

It's not recommended to reinvent the wheel by implementing custom certificate chain validation.

TLS libraries provide built-in certificate validation functions that should be used.

Noncompliant Code Example

`checkClientTrusted` and/or `checkServerTrusted` custom implementations from `X509TrustManager` interface accept any certificates:

```
// Create a trust manager that does not validate certificate chains
val trustAllCerts = arrayOf<TrustManager>(object :
X509TrustManager {
  @Throws(CertificateException::class)
   override fun checkClientTrusted(chain:
Array<java.security.cert.X509Certificate>, authType: String) {
  } // Noncompliant (s4830)

  @Throws(CertificateException::class)
    override fun checkServerTrusted(chain:
Array<java.security.cert.X509Certificate>, authType: String) {
   } // Noncompliant (s4830)

  override fun getAcceptedIssuers():
Array<java.security.cert.X509Certificate> {
   return arrayOf()
  }
 })

// Install the all-trusting trust manager
val sslContext = SSLContext.getInstance("SSL")
sslContext.init(null, trustAllCerts, java.security.SecureRandom())
```

Compliant Solution

By default, when a `TrustManager` is not set, `sslContext` will search for a default secure installed security provider:

```
val sslContext = SSLContext.getInstance("SSL")
sslContext.init(null, null, java.security.SecureRandom())
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- Mobile AppSec Verification Standard - Network Communication Requirements
- OWASP Mobile Top 10 2016 Category M3 - Insecure Communication

- MITRE, CWE-295 - Improper Certificate Validation