

# eMudhra certificate compromise: GraalVM Native Image advisory

Native Image captures the default trust store and certificate blocklist at build time. Updating the JDK or replacing its `lib/security/blocked.certs` file does not update an existing native executable. See [Certificate Management in Native Image](#) for details on build-time capture and runtime trust-store overrides.

## Option 1: Update the build environment and rebuild

Download the fixed GraalVM distribution from [GraalVM downloads](#), then rebuild and redeploy affected native executables. Alternatively, apply the advisory's manual blocklist replacement to the JDK used by Native Image, preserving any custom blocklist entries, then rebuild and redeploy. Oracle's advisory instructs Java 8 users to rename `blocked.certs` to `blacklisted.certs`; use the filename expected by the JDK used for the build. This incorporates the updated blocklist into the executable and rejects the listed compromised certificates without removing trust in unrelated certificates issued under the same roots.

## Option 2: Override the trust store without rebuilding (expert option)

For applications using the default Java TLS trust manager, an existing native executable can use a replacement trust store at startup:

```
./application \

-Djavax.net.ssl.trustStore=/absolute/path/hotfix-truststore.p12 \

-Djavax.net.ssl.trustStoreType=PKCS12
```

Prepare the replacement store from the application's intended trusted certificates, removing every trust anchor that could validate the compromised intermediates. This includes the **emSign Root TLS CA - G3** and **emSign ECC Root CA - G3** roots used by the reported eMudhra chains, and the **AAA Certificate Services** root used by a cross-signed path, as well as any directly trusted intermediate that provides another validation path.

Merely omitting the compromised intermediates is insufficient: a peer can supply them during the TLS handshake if a trusted root still validates the chain.

Restart the application with the replacement store. No rebuild is required for this option. However:

- The replacement store replaces, rather than supplements, the embedded default trust store.
- Removing roots can also reject legitimate certificates chaining to those roots.
- This override does not update the executable's embedded certificate blocklist.

## Option 3: Enable and verify revocation checking

The [Oracle Java advisory](#) describes enabling TLS revocation checking with:

```
-Dcom.sun.net.ssl.checkRevocation=true

-Dcom.sun.security.enableCRLDP=true
```

For Native Image, do not assume that adding these flags to an existing executable is sufficient. Relevant settings may have been captured during build-time class initialization. Before relying on this option, confirm that the executable rejects the affected chains and that revocation checking behaves appropriately when revocation information is unavailable.

## Validate the remediation

GraalVM Native Image applications using Java TLS certificate validation may trust certificate chains containing the compromised eMudhra intermediate CA certificates. Oracle's [Java advisory](#) describes the incident and provides JDK updates and mitigation options. Test rejection against the incident's test endpoints. Two published examples cover the eMudhra and AAA cross-signed paths:

- [eMudhra cross-signed test endpoint](#)
- [AAA cross-signed test endpoint](#)

Configure a test instance of the native image application to request these URLs without credentials or application data. A certificate validation error indicates that the client does not trust the compromised intermediates. The [incident site](#) also provides `chains.zip`, covering all twelve TLS test hosts. The two URLs above are a spot check, not complete coverage.

The options described above apply to applications using Java's default TLS trust infrastructure. Applications using custom trust managers, independently configured TLS contexts, or separate native TLS libraries require assessment and remediation of those configurations.

See the [Oracle Java advisory](#) for the replacement blocklist and JDK remediation instructions.