











com/thoughtworks/go/config/ materials/MaterialConfigs.java	280	2	SECURITY	HARD_CODE_PASSWORD	 
	289	2	SECURITY	HARD_CODE_PASSWORD	 
com/thoughtworks/go/security/ X509CertificateGenerator.java	214	1	SECURITY	HARD_CODE_PASSWORD	 
	243	1	SECURITY	HARD_CODE_PASSWORD	 
	245	1	SECURITY	HARD_CODE_PASSWORD	 

```

public SvnMaterialConfig getSvnMaterial() {
    SvnMaterialConfig svnMaterialConfig = new SvnMaterialConfig();
    svnMaterialConfig.setUrl("");
    svnMaterialConfig.setUserName("");
    svnMaterialConfig.setPassword("");
    svnMaterialConfig.setCheckExternals(false);
    return getExistingOrDefaultMaterial(svnMaterialConfig);
}

public TfsMaterialConfig getTfsMaterial() {
    TfsMaterialConfig tfsMaterialConfig = new TfsMaterialConfig();
    tfsMaterialConfig.setUrl("");
    tfsMaterialConfig.setUserName("");
    tfsMaterialConfig.setPassword("");
    tfsMaterialConfig.setProjectPath("");
    return getExistingOrDefaultMaterial(tfsMaterialConfig);
}

public HgMaterialConfig getHgMaterial() {
    HgMaterialConfig hgMaterialConfig = new HgMaterialConfig();
    hgMaterialConfig.setUrl("");
    return getExistingOrDefaultMaterial(hgMaterialConfig);
}

public GitMaterialConfig getGitMaterial() {
    GitMaterialConfig gitMaterialConfig = new GitMaterialConfig();
    gitMaterialConfig.setUrl("");
    return getExistingOrDefaultMaterial(gitMaterialConfig);
}
"config/config-api/src/main/java/com/thoughtworks/go/config/materials/MaterialConfigs.java" 405L, 16453C
280,42

```

```

// Load the keystore
boolean verifySigned(File keystore, Certificate agentCertificate) {
    try {
        KeyStore store = KeyStore.getInstance("JKS");
        try (FileInputStream inputStream = new FileInputStream(keystore)) {
            store.load(inputStream, PASSWORD_AS_CHAR_ARRAY);
        }
        KeyStore.PrivateKeyEntry intermediateEntry = (KeyStore.PrivateKeyEntry) store.getEntry("ke-intermediate",
            new KeyStore.PasswordProtection(PASSWORD_AS_CHAR_ARRAY));
        Certificate intermediateCertificate = intermediateEntry.getCertificate();
        agentCertificate.verify(intermediateCertificate.getPublicKey());
        return true;
    } catch (Exception e) {
        return false;
    }
}

private String getHostname() {
    try {
        return InetAddress.getLocalHost().getHostName();
    } catch (UnknownHostException e) {
        throw bomb(e);
    }
}

private BigInteger serialNumber() {
    return new BigInteger(Long.toString(Math.round(Math.random() * 512048976484480)));
}

private KeyPair generateKeyPair() {

```

"common/src/main/java/com/thoughtworks/go/security/X509CertificateGenerator.java" 310L, 14150C 243,64

Hard coded password found

Passwords should not be kept in the source code. The source code can be widely shared in an enterprise environment, and is certainly shared in open source. To be managed safely, passwords and secret keys should be stored in separate configuration files or keystores. (Hard coded keys are reported separately by Hard Coded Key pattern)

Vulnerable Code:

```

private String SECRET_PASSWORD = "letMeIn!"; Properties props = new Properties();
props.put(Context.SECURITY_CREDENTIALS, "p@ssw0rd");

```

References

CWE-259: Use of Hard-coded Password