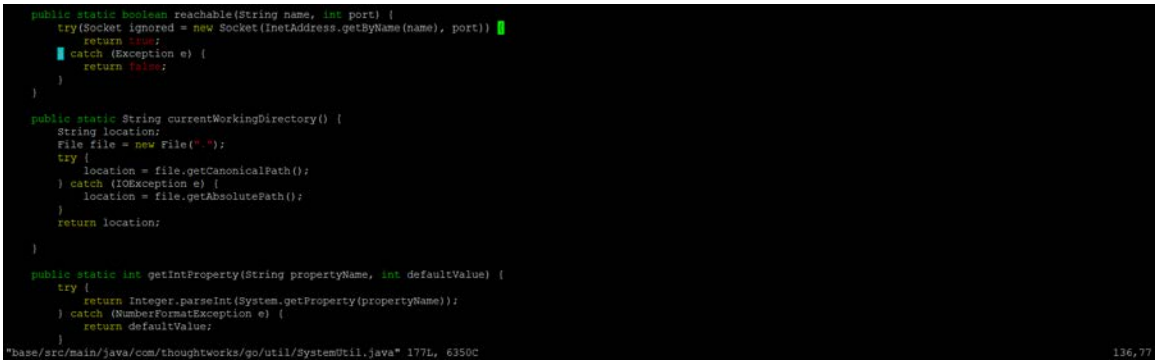
com/thoughtworks/go/util/SystemUtil.java	136	2	SECURITY	UNENCRYPTED_SOCKET



Unencrypted socket to com.thoughtworks.go.util.SystemUtil (instead of SSLSocket)

The communication channel used is not encrypted. The traffic could be read by an attacker intercepting the network traffic.

Vulnerable Code:

Plain socket (Cleartext communication):

Socket soc = new Socket("www.google.com",80);

Solution:

SSL Socket (Secure communication):

Socket soc = SSLSocketFactory.getDefault().createSocket("www.google.com", 443);

Beyond using an SSL socket, you need to make sure your use of SSLSocketFactory does all the appropriate certificate validation checks to make sure you are not subject to man-in-the-middle attacks. Please read the OWASP Transport Layer Protection Cheat Sheet for details on how to do this correctly.

References

OWASP: Top 10 2010-A9-Insufficient Transport Layer Protection

OWASP: Top 10 2013-A6-Sensitive Data Exposure

OWASP: Transport Layer Protection Cheat Sheet

WASC-04: Insufficient Transport Layer Protection

CWE-319: Cleartext Transmission of Sensitive Information