Security Findings of Project "1BadHostNameVerifier"

Analysis Date: 2020-03-13 08:21:43

Analyzed Workspace:

Packages:	1	Total LOC:	16
Classes:	2	No. of Bytecode Instructions:	21

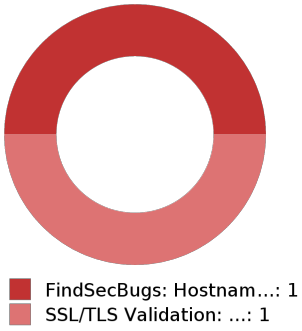
Computed Call Graph:

Classes not in Call Graph:	0	Methods not in Call Graph:	0

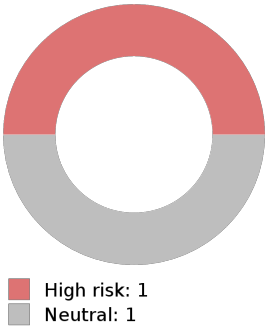
Findings in List:

All Findings:	2	Problematic Findings:	2

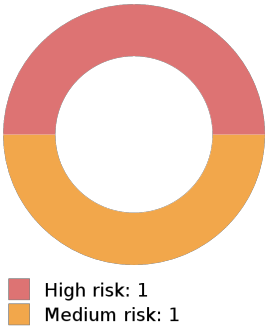
Finding Problem Types:



Finding Classifications:

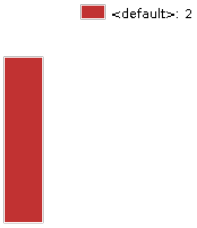


Finding Ratings:

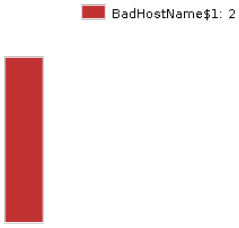


OWASP Top 10 2017

Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	**1**	**Problem Type:**	FindSecBugs: HostnameVerifier that accept any signed certificates (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-03-13 08:21:43 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	BadHostName.java (<Source Code>):12		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: HostnameVerifier that accept any signed certificates makes communication vulnerable to a MITM attack - In method BadHostName$1.verify(String, SSLSession)		

Finding ID:	**2**	**Problem Type:**	SSL/TLS Validation: Suspicious Implementation (Special Code)
Classification:	Manual Review Required	**Date:**	2020-03-13 08:21:43 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	BadHostName.java (<Source Code>):10		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'SSL/TLS Validation: Suspicious Implementation'. Matching pattern in special code kind 'SSL/TLS Validation: Suspicious Implementation': boolean javax.net.ssl.HostnameVerifier.verify(java.lang.String, javax.net.ssl.SSLSession)		