

Security Findings of Project "5BadHostnameVerifierWithGenericCondition"

Analysis Date: 2020-06-04 10:29:28

Analyzed Workspace:

Packages:	1	Total LOC:	20
Classes:	3	No. of Bytecode Instructions:	26

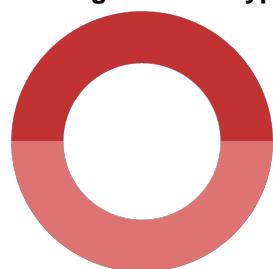
Computed Call Graph:

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

Findings in List:

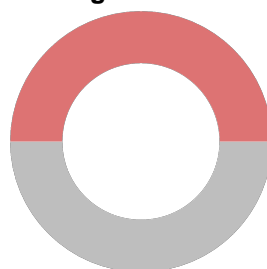
All Findings:	2	Problematic Findings:	2
---------------	---	-----------------------	---

Finding Problem Types:



FindSecBugs: Hostnam...: 1
SSL/TLS Validation: ...: 1

Finding Classifications:



High risk: 1
Neutral: 1

Finding Ratings:

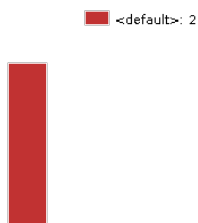


High risk: 1
Medium risk: 1

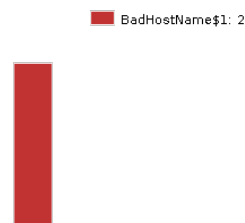
OWASP Top 10 2017



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:	2020-06-04 10:29:28 - new
Rating:	8.00	Reviewed State:	Not Reviewed
Location:	BadHostName.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
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:	2020-06-04 10:29:28 - new
Rating:	4.00	Reviewed State:	Not Reviewed
Location:	BadHostName.java (<Source Code>):7		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
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)		