

## Security Findings of Project "5BareBone X509TrustManagerCanBypass"

**Analysis Date:** 2020-03-05 08:18:50

### Analyzed Workspace:

|           |   |                               |    |
|-----------|---|-------------------------------|----|
| Packages: | 1 | Total LOC:                    | 38 |
| Classes:  | 3 | No. of Bytecode Instructions: | 42 |

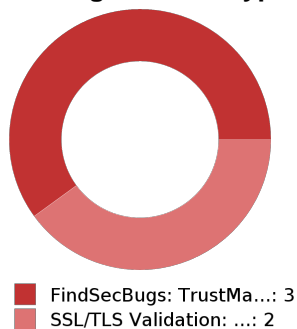
### Computed Call Graph:

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

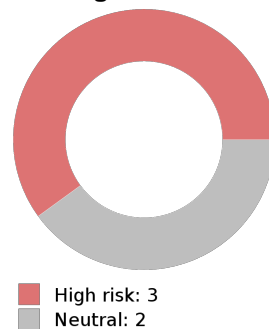
### Findings in List:

|               |   |                       |   |
|---------------|---|-----------------------|---|
| All Findings: | 5 | Problematic Findings: | 5 |
|---------------|---|-----------------------|---|

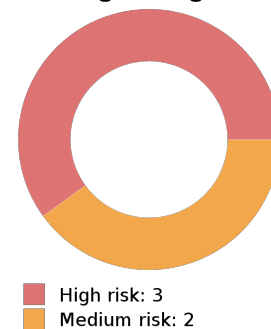
#### Finding Problem Types:



#### Finding Classifications:



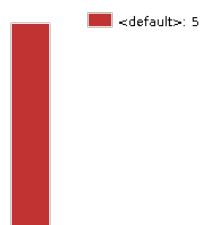
#### Finding Ratings:



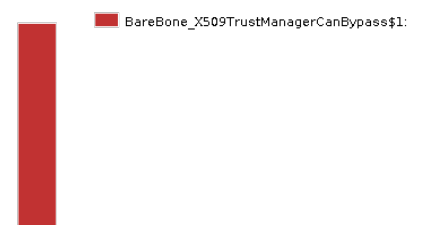
#### OWASP Top 10 2017



#### Hot Spots (Packages)



#### Hot Spots (Classes)



## Findings List

|                        |   |                        |   |
|------------------------|---|------------------------|---|
| <b>Finding ID:</b>     | 1   | <b>Problem Type:</b>   | FindSecBugs: TrustManager that accept any certificates (SpotBugs Security Issues) |
| <b>Classification:</b> | Warning   | <b>Date:</b>           | 2020-03-05 08:18:50 - new   |
| <b>Rating:</b>         | 8.00  | <b>Reviewed State:</b> | Not Reviewed  |
| <b>Location:</b>       | BareBone_X509TrustManagerCanBypass.java (<Source Code>):14  |                        |   |
| <b>Tags:</b>           | no tags assigned  |                        |   |
| <b>Comment:</b>        | no comment  |                        |   |
| <b>Description:</b>    | <p>A finding identified by the external 'SpotBugs' plugin:<br/>TrustManager that accept any certificates makes communication vulnerable to a MITM attack</p> <p>- In method BareBone_X509TrustManagerCanBypass\$1.checkClientTrusted(X509Certificate[], String)</p> |                        |   |

|                        |   |                        |   |
|------------------------|---|------------------------|---|
| <b>Finding ID:</b>     | 2   | <b>Problem Type:</b>   | FindSecBugs: TrustManager that accept any certificates (SpotBugs Security Issues) |
| <b>Classification:</b> | Warning   | <b>Date:</b>           | 2020-03-05 08:18:50 - new   |
| <b>Rating:</b>         | 8.00  | <b>Reviewed State:</b> | Not Reviewed  |
| <b>Location:</b>       | BareBone_X509TrustManagerCanBypass.java (<Source Code>):20  |                        |   |
| <b>Tags:</b>           | no tags assigned  |                        |   |
| <b>Comment:</b>        | no comment  |                        |   |
| <b>Description:</b>    | <p>A finding identified by the external 'SpotBugs' plugin:<br/>TrustManager that accept any certificates makes communication vulnerable to a MITM attack</p> <p>- In method BareBone_X509TrustManagerCanBypass\$1.checkServerTrusted(X509Certificate[], String)</p> |                        |   |

|                        |  |                        |   |
|------------------------|--|------------------------|---|
| <b>Finding ID:</b>     | 3  | <b>Problem Type:</b>   | FindSecBugs: TrustManager that accept any certificates (SpotBugs Security Issues) |
| <b>Classification:</b> | Warning  | <b>Date:</b>           | 2020-03-05 08:18:50 - new   |
| <b>Rating:</b>         | 8.00   | <b>Reviewed State:</b> | Not Reviewed  |
| <b>Location:</b>       | BareBone_X509TrustManagerCanBypass.java (<Source Code>):25   |                        |   |
| <b>Tags:</b>           | no tags assigned   |                        |   |
| <b>Comment:</b>        | no comment   |                        |   |
| <b>Description:</b>    | <p>A finding identified by the external 'SpotBugs' plugin:<br/>TrustManager that accept any certificates makes communication vulnerable to a MITM attack</p> <p>- In method BareBone_X509TrustManagerCanBypass\$1.getAcceptedIssuers()</p> |                        |   |

### Findings List

|                        |  |                        |  |
|------------------------|--|------------------------|--|
| <b>Finding ID:</b>     | <b>4</b>   | <b>Problem Type:</b>   | SSL/TLS Validation: Suspicious Implementation (Special Code) |
| <b>Classification:</b> | Manual Review Required   | <b>Date:</b>           | 2020-03-05 08:18:50 - new                                    |
| <b>Rating:</b>         | 4.00   | <b>Reviewed State:</b> | Not Reviewed   |
| <b>Location:</b>       | BareBone_X509TrustManagerCanBypass.java (<Source Code>):11   |                        |  |
| <b>Tags:</b>           | no tags assigned   |                        |  |
| <b>Comment:</b>        | <i>no comment</i>  |                        |  |
| <b>Description:</b>    | An identified location for problem type 'SSL/TLS Validation: Suspicious Implementation'.<br><br>Matching pattern in special code kind 'SSL/TLS Validation: Suspicious Implementation':<br>void javax.net.ssl.X509TrustManager.checkClientTrusted(java.security.cert.X509Certificate[], java.lang.String) |                        |  |

|                        |  |                        |  |
|------------------------|--|------------------------|--|
| <b>Finding ID:</b>     | <b>5</b>   | <b>Problem Type:</b>   | SSL/TLS Validation: Suspicious Implementation (Special Code) |
| <b>Classification:</b> | Manual Review Required   | <b>Date:</b>           | 2020-03-05 08:18:50 - new                                    |
| <b>Rating:</b>         | 4.00   | <b>Reviewed State:</b> | Not Reviewed   |
| <b>Location:</b>       | BareBone_X509TrustManagerCanBypass.java (<Source Code>):17   |                        |  |
| <b>Tags:</b>           | no tags assigned   |                        |  |
| <b>Comment:</b>        | <i>no comment</i>  |                        |  |
| <b>Description:</b>    | An identified location for problem type 'SSL/TLS Validation: Suspicious Implementation'.<br><br>Matching pattern in special code kind 'SSL/TLS Validation: Suspicious Implementation':<br>void javax.net.ssl.X509TrustManager.checkServerTrusted(java.security.cert.X509Certificate[], java.lang.String) |                        |  |