**Transport layer without the use of encryption**

**SEVERITY:** **MODERATE**

**VULN. CODE:** NOCRYPTT

**AUTH. REQUIRED:** NO

**VULNERABILITY DESCRIPTION**

Insufficient protection of the transport layer exposes communications to an attacker, allowing an attack vector to compromise a web application and/or extract sensitive information. In particular, unencrypted connections allow interception, injection and redirection (also known as man in the middle/MiTM attacks). An attacker may passively intercept communication to obtain information about the systems they are communicating and may be able to actively inject/remove content from the communication to forge or omit information, insert malicious scripting, or redirect the client to untrusted content. Similarly, the attacker will be able to redirect the communication so that the web application and the client are no longer able to exchange information directly, but through the attacker, and believing they are communicating in a trusted way.

Responses coming from HTTP service without using any TLS/SSL protocol have been logged.

**SUGGESTED SOLUTIONS**

It is recommended to implement encryption mechanisms to protect all communications between the client and the server after the authentication process. If encryption mechanisms cannot be enabled to protect all communications after authentication, it is recommended to protect at least communications related to sensitive processes. Communications to be protected include all communications related to the authentication process and its related functionalities, functionalities where sensitive data is manipulated for the application or which allow the execution of operations of an administrative nature. In particular, it is recommended, first of all, to disable the data transfer mode via HTTP, and secondly to consider the use of an encrypted exchange protocol, such as HTTPS through the correct configuration of SSL certificates.

**REFERENCES**

More information regarding the vulnerability and its possible solutions can be found on the following addresses:

**REF 20 – www.owasp.org/index.php/OWASP\_Application\_Security\_FAQ**

**REF 21 – cwe.mitre.org/data/definitions/311.html**

**REF 22 – cwe.mitre.org/data/definitions/523.html**

**REF 23 – cwe.mitre.org/data/definitions/319.html**

**REF 24 – projects.webappsec.org/w/page/13246945/Insufficient Transport Layer Protection**