**Lack of protection mechanisms against Clickjacking attacks**

**SEVERITY:** **MODERATE**

**VULN. CODE:** CJK-PROT

**AUTH. REQUIRED:**

**VULNERABILITY DESCRIPTION**

Clickjacking is an attack that allows a threat agent to control the actions performed by the user within a WEB application. The most common attack is performed through the use of an IFRAMEs injected on the original site which can trick the user into performing unwanted actions in an unconscious manner. This technique can also be used to circumvent the protection mechanisms against XSRF attacks. During the analysis activity, no countermeasures were detected that could prevent this type of vulnerability, either within the HTTP headers, or within the HTML generated by the application (framebusting).

Below the evidence of the clickjacking vulnerability and the lack of the X-Frame-Options header.

|  |
| --- |
| **RESPONSE**  HTTP/1.1 200 OK  Date: Fri, 21 Feb 2020 10:32:29 GMT  Content-Type: text/html  Connection: close  Vary: Accept-Encoding  Last-Modified: Thu, 09 Jan 2020 03:16:01 GMT  Content-Length: 2150 |

**Box 5 – Lack of X-Frame-Options Header**

**SUGGESTED SOLUTIONS**

It is advisable to check the functionalities of the application that carry out privileged operations, and that are therefore accessible following the authentication process, in order to implement the appropriate prevention mechanisms for attacks related to this category. Among the various attack prevention techniques, it is recommended to use the X-Frame-Options entry inside the header to adjust the use of frames within the application context. If it is not possible to implement the protection inside the header it is recommended to implement “framebusting” mechanisms within the HTML generated by the application.

The X-Frame-Options header will be interpreted by the end user's browser and will automatically prevent the user browser from rendering external sites, automatically called within an IFRAME by pages properly constructed for the purpose of fraud and / or other malicious uses.

|  |
| --- |
| X-Frame-Options: SAMEORIGIN |

**REFERENCES**

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

**REF 16 – www.owasp.org/index.php/Clickjacking  
REF 17 – support.microsoft.com/kb/2694329  
REF 18 – developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options  
REF 19 – tools.ietf.org/html/rfc7034**