CROSS SITE VULNERABILTIY FOR NON-TECHIES

INTRODUCTION

This document is to provide more help to non-techies who encounter this problem. If you need more help than what TEC567263 provides, please read on.

THE PROBLEM

Clarity has vulnerability for Cross site forgery attacks in versions prior to v12.1.3 and v13.0 prior to v13.0.2

In v12.1.3 and v13.1 there is a solution applied for this. The solution in those version may cause the users getting an error while navigating in Clarity.

See the latest version of **TEC567263 Clarity has a vulnerability to Cross Site Request Forgery (CSRF) Attacks** in support site knowledge base.

IN PRACTISE

If you have v12.1.3 or v.13.1 you can totally override the CSRF protection. See the above mentioned TECH DOC.

You recognize this problem if you get

Clarity PPM 12.1.3: " ERROR 500 - Internal Server Error"

Clarity PPM 13.1: "Security Violation: CSRF Attack" followed by instructions on what caused the error and what to do to recover.

Ii both cases you can check the app-niku.log/app-ca.log

If you are On Demand do as the TECH DOC says, contact support, because you do not have the required access.

ADDITIONAL DETAILS FOR NON-TECHIES

If you are on premise and do not want to totally override the CSRF protection, TEC567263 provides instructions how to add specific exceptions to the CSRF protection.

First you have to recognize that the error you get is from the CSRF protection: see the app-niku.log/app-ca.log.

Then get CMN_OPTION_EXEMPTED_ACTION_VALUES.xml either as the TECH DOC says delivered as part of the 12.1.3 patch or get it from the support. The latter means that there is a link to it in the TECH DOC and you can get it from the link and don't have to open a case for that.

The TECH DOC further instructs what to do with the CMN_OPTION_EXEMPTED_ACTION_VALUES.xml and how to install that.

Note the in MS SQL server you have to login in as the same user which is specified in NSA/CSA otherwise you get an error

'Could not find stored procedure 'CMN_ID_SP'

When you get past that error and get

'Argument data type numeric is invalid for argument 2 of substring function.'

you cannot use the proposed method, but have to take a shortcut and use

EXEC CMN_OPTION_VALUES_INS_SP 'CSRF_EXEMPTED_ACTIONS', null, null, 'the name of the action from app-niku.log', 1

instead

When you are done restart the app service and the users should clear their browser caches.

WHAT ACTUALLY HAPPENS IN NON-TECHIE TERMS

This is a simplified explanation

The CSRF vulnerability prevention functions with cached tokens. Sometimes when the user navigates the required token is not cached and therefore the ERROR 5000. Sometimes simply refreshing the page will reload the page and get a new token and let the user continue. If that does not happen an exception has to be created.

v12.1.3 patch has for that purpose the value CSRF_EXEMPTED_ACTIONS in CMN_OPTIONS.OPTION_CODE. If that is there the system is ready for exceptions.

An exception is needed for basically every action that gives the ERROR 5000 and has 'The request could not be completed due to a conflict with the current state of the resource' in the log. In practice you should start with the most frequent and consistent ones. The method described in the TECH DOC adds an exception a value is written to CMN_OPTION_VALUES.VALUE.

Use this query to verify that your system is ready for the exceptions and what exceptions have been made.

select '@@' + value + '@@' as exemption_value from niku.cmn_option_values where option_id in

(select id from niku.cmn_options where option_code ='CSRF_EXEMPTED_ACTIONS')

MORE INFO

In addition to the TECH DOC there is some discussion in the thread 'scanning clarity installation: cross site forgery request' on Clarity General Discussion message board.

VERSION

Version 1.0 April 1, 2013 MKi

DISCLAIMER