[WSO2]

WSO2 API Manager 2.6.0 - CVE-2020-17454

- Author : Zakaria BRAHIMI
- Published: 12th October 2020
- Severity: Medium
- CVSS Score: 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

AFFECTED PRODUCTS

WSO2 API Manager: 3.1.0 or earlier

OVERVIEW

Self Cross-Site Scripting (XSS) vulnerability in the API Manager Admin Portal.

DESCRIPTION

Self Cross-Site Scripting (XSS) vulnerability can be exploited when changing the application owner by sending a request with a malicious payload.

IMPACT

By leveraging the Self Cross-Site Scripting (XSS) vulnerability in the API Manager Admin Portal, an attacker could persuade an admin user using Social Engineering to submit a malicious payload and get the user redirected to an attacker controlled page where a phishing attack could be executed to obtain highly sensitive information or conduct further attacks against the victim.

SOLUTION

If you are using an affected product version, it is highly recommended to migrate to the latest released version to receive security fixes.

You may also apply the relevant fixes based on the changes from the public fix:
https://github.com/wso2/carbon-apimgt/pull/9011

POC

The POST parameter **owner** allowing to specify the owner of an application is sensitive to reflected XSS injections. Although a filter allowing to verify the veracity of the owner name provided against users existing in the database are in place, nevertheless, at the time of validation of the form, just after modifying the owner name, a modal box appears which specify, in case of error, that the inputted value could not be assigned to the **owner** parameter. This avoids a stored XSS type vulnerability, of course, however the value entered is displayed as it is inside the modal box ; which leads to the presence of a reflected XSS vulnerability due to the absence of filtering on the POST 'owner' parameter.

To illustrate these words, I first injected an HTML code allowing to write a title (using the HTML tag <h3>) as follows:

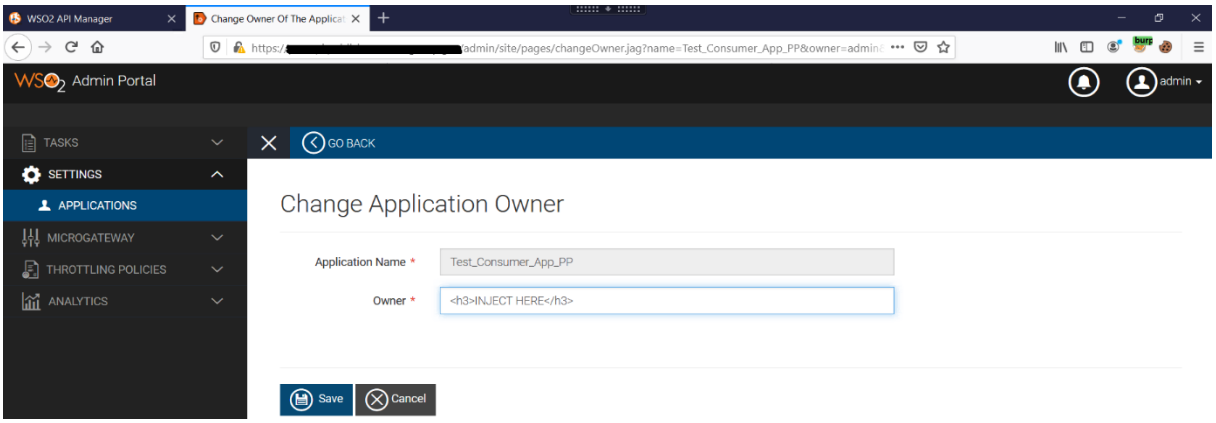

Figure 1: Injection point

The HTML code is interpreted and displayed in the modal box without constraint, as follows:

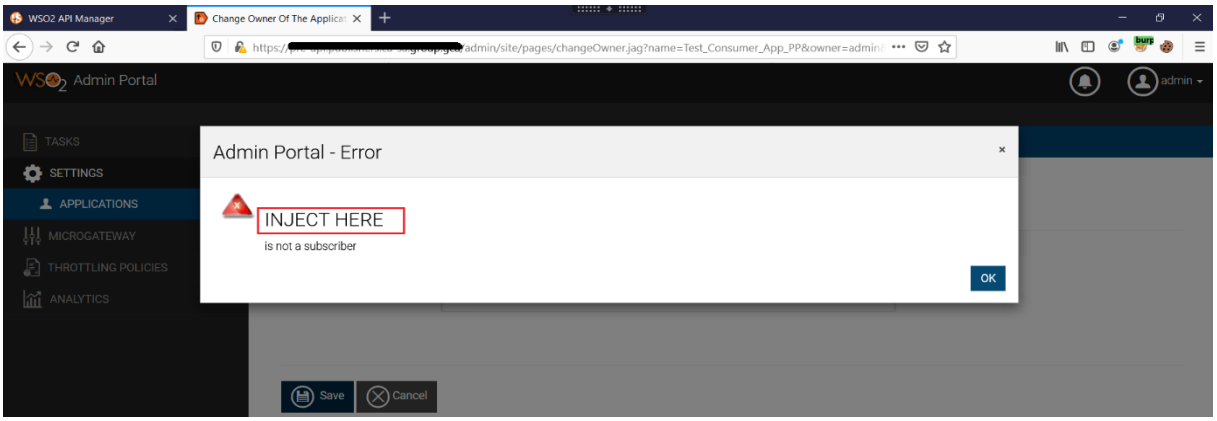

Figure 2: HTML code injection

From there, the doubt about the presence of a possible XSS is raised. In the absence of filtering of HTML entities in the returned error message, I tried to inject a basic XSS payload (without any form of bypass) allowing to arise a dialog box (alert) in the browser. It turns out that the result was conclusive. The following capture attests to this fact:

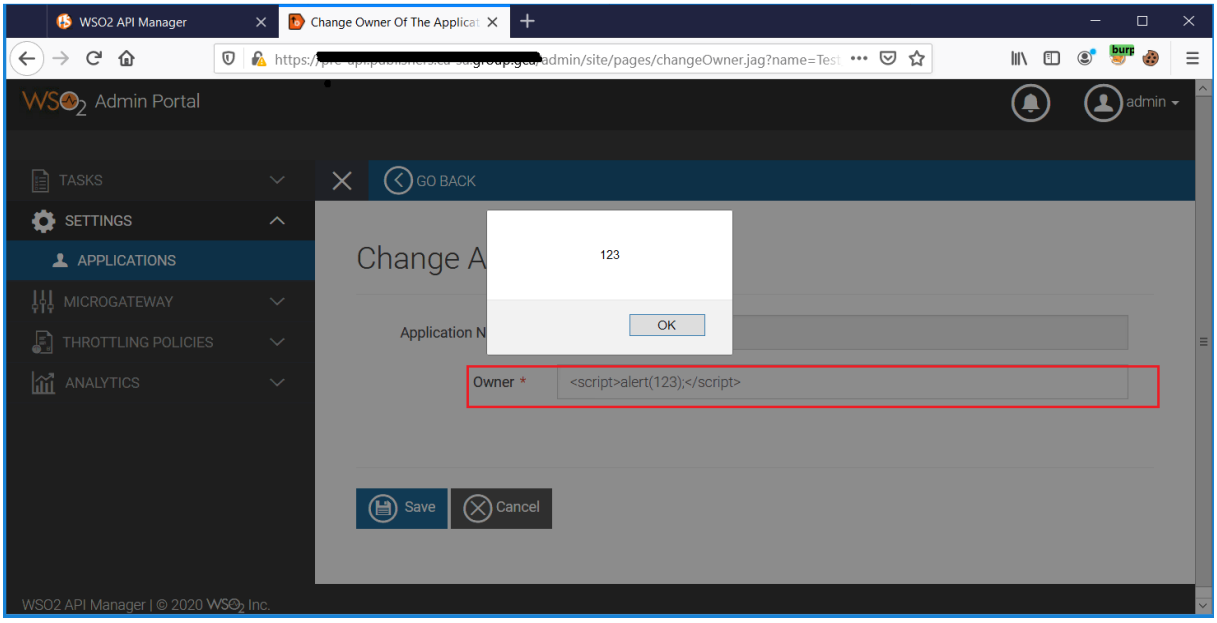

Figure 3: XSS Injection

A second XSS payload was tested. This time a JavaScript code allowing to write in the current document was used. The result is illustrated in the following screenshots:

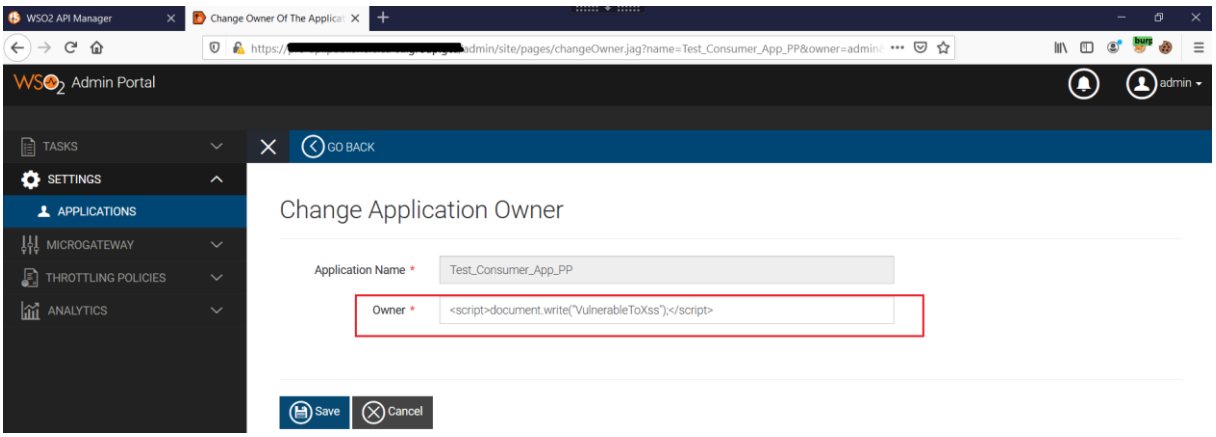

Figure 4: Another XSS injection

Similarly, the script is reflected in output without constraint, which confirms the presence of the vulnerability as follows:

Figure 5: XSS execution

The vulnerability has been tested through a Google Chrome browser from a Windows system but remains exploitable on other browsers and systems.

Criticality and exploitability

The criticality of the vulnerability was rated as **medium** for several reasons. Indeed, several conditions are necessary for the exploitation of this vulnerability. First you need to have an administrator account to connect to the admin area of the WSO2 API Manager. Also, since the XSS is not stored, the injection performed is not preserved by the application; therefore the attack should be targeted and it is not possible to harm multiple administrators in one shot.

Besides, exploitation of this vulnerability is difficult because to achieve this, the attacker must push the victim to a hostile domain where a forged http request will be launched, by the victim's browser to the vulnerable application. This request must be correctly forged with the good POST parameters in addition to the XSS injection payload. For these reasons, the impact and criticality of the vulnerability have been reduced.

References

- **https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0843**
- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17454**
- **https://nvd.nist.gov/vuln/detail/CVE-2020-17454**