Talos Vulnerability Report

TALOS-2020-1198

Rukovoditel Project Management App SQL injection vulnerability in the 'forms_fields_rules/rules' page

APRIL 8, 2021

CVE NUMBER

CVE-2020-13587

Summary

An exploitable SQL injection vulnerability exists in the ‘forms_fields_rules/rules’ page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.

Tested Versions

Rukovoditel Project Management App 2.7.2

Product URLs

https://www.rukovoditel.net/

CVSSv3 Score

5.4 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N

CWE

CWE-89 - Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)

Details

Rukovoditel is an open-source project management tool and CRM tool designed to support project managers in complex tasks.

The `id` parameter in the `forms_fields_rules/rules` page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /crm/index.php?module=forms_fields_rules/rules&action=get_fields_choices&id=1<SQLINJECTION>&fields_id=1 HTTP/1.1
Host: [IP]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html, */*; q=0.01
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/crm/index.php?module=entities/forms&entities_id=24
Cookie: cookie_test=please_accept_for_session; sid=84edp91galu92kc98ja9r4uhto; PHPSESSID=hru4oem2h86lj609i2acmvrnup
Content-Type: application/x-www-form-urlencoded
Content-Length: 18

selected_fields=1
```

The above SQL injection exist in the `forms_fields_rules/rules` page due to lack of filtering applied on the specific parameter. Below is the source code which shows the SQL vulnerability injection: at line 72 the unsanitized `id` is used as part of select query.

56 case ‘get_fields_choices’:

```
 57
 58                 if(isset($_GET['id']))
 59                 {
 60                         $obj = db_find('app_forms_fields_rules',$_GET['id']);
 61                 }
 62                 else
 63                 {
 64                         $obj = db_show_columns('app_forms_fields_rules');
 65                 }
 66
 67                 $fields_id = _get::int('fields_id');
 68
 69                 $field_info = db_find('app_fields', $fields_id);
 70
 71                 $exclude_choices = array();
 72                 $rules_query = db_query("select * from app_forms_fields_rules where fields_id='" . $fields_id . "'" .
(isset($_GET['id']) ? " and id!='" . $_GET['id']. "'":''));
 73                 while($rules = db_fetch_array($rules_query))
 74                 {
 75                         if(strlen($rules['choices']))
 76                         {
 77                                 $exclude_choices = array_merge($exclude_choices,explode(',',$rules['choices']));
 78                         }
```

An attacker either needs administrator privileges or they could trigger this vulnerability through cross-site request forgery.

Timeline

2020-11-24 - Vendor Disclosure
2021-02-09 - 60+ day follow up
2021-02-10 - Vendor advises issue not a security vulnerability
2021-02-23 - Talos retested and reconfirmed security vulnerability on new version 2.8.2 and provided to vendor
2021-03-03 - 90 day follow up
2021-04-08 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2020-1199

NEXT REPORT
TALOS-2021-1247