Talos Vulnerability Report

TALOS-2020-1201

Rukovoditel Project Management App application SQL injection vulnerability in the 'global_lists/choices' page

APRIL 8, 2021

CVE NUMBER

CVE-2020-13592

Summary

An exploitable SQL injection vulnerability exists in ‘global_lists/choices’ 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 `lists_id` parameter in the “global_lists/choices” page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /crm/index.php?module=global_lists/choices&fields_id=1&entities_id=1&lists_id=1<SQLINJECTION> 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: 3

a=1
```

The above SQL injection exist in the “global_lists/choices” page due to lack of filtering applied on the `lists_id` parameter. At line 10 we can see that an unsanitized `lists_id` is used as part of `select` query.

```
 3 require('includes/libs/PhpSpreadsheet-master/vendor/autoload.php');
 4
 5 use PhpOffice\PhpSpreadsheet\Spreadsheet;
 6 use PhpOffice\PhpSpreadsheet\Writer\Xlsx;
 7 use PhpOffice\PhpSpreadsheet\IOFactory;
 8
 9
10 $list_info_query = db_query("select * from app_global_lists where id='" . $_GET['lists_id']. "'");
11 if(!$list_info = db_fetch_array($list_info_query))
12 {
13   redirect_to('global_lists/lists');
```

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 is not a security vulnerability

2021-02-23 - Talos retested and reconfirmed on new version 2.8.2; follow up email issued to vendor

2021-03-03 - 3rd follow up and final 90 day notice; vendor unresponsive 2021-04-08 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.