Talos Vulnerability Report

TALOS-2020-1126

ProcessMaker sort parameter multiple SQL Injection Vulnerabilities

NOVEMBER 17, 2020

CVE NUMBER

CVE-2020-13525, CVE-2020-13526

Summary

Multiple SQL injection vulnerabilities exist in the handling of sort parameters in ProcessMaker 3.4.11. A specially crafted HTTP request can cause an SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.

Tested Versions

ProcessMaker 3.4.11

Product URLs

https://www.processmaker.com/

CVSSv3 Score

6.4 - CVSS:3.0/AV:N/AC:L/PR:L/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

ProcessMaker is a software suite used for workflow management. It can be used to automate workflow, create documents, assign roles and users to processes and more

It has an open-source community version and a commercial version. It is used by many large companies such as Airbus, Sony and Bridgestone.

The `reportTables_Ajax` and `clientSetupAjax` pages are vulnerable to SQL injection in the `sort` parameter.

CVE-2020-13525 - reportTables_Ajax page

The `sort` parameter in the download page `/sysworkflow/en/neoclassic/reportTables/reportTables_Ajax` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
POST /sysworkflow/en/neoclassic/reportTables/reportTables_Ajax HTTP/1.1
Host: [IP]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 82
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/sysworkflow/en/neoclassic/processes/mainInit
Cookie: PM-
Warning=Warning%3A+Processmaker+does+not+permit+you+to+open+multiple+tabs+in+the+same+browser+session+because+of+security+restrictions.++Thi
s+page+will+be+closed.; workspaceSkin=neoclassic; PHPSESSID=ja3jegutcirelr3g3tid62tcoq; PM-TabPrimary=101010010; singleSignOn=0

start=0&limit=20&option=UPD&pageSize=20&search=&sort=[SQL INJECTION]&action=list&dir=1
```

The `sort` parameter is passed to 'reportTables_Ajax.php' on line 304 before being passed to AdditionalTables function which eventually being used as part of an `ORDER BY` query in 'workflow/engine/classes/model/om/BaseAdditionalTablesPeer.php' source file at line 353.

```
297         $limit = isset( $_REQUEST['limit'] ) ? $_REQUEST['limit'] : $limit_size;
298         $filter = isset( $_REQUEST['textFilter'] ) ? $_REQUEST['textFilter'] : '';
299         $pro_uid = isset( $_REQUEST['pro_uid'] ) ? $_REQUEST['pro_uid'] : '';
300
301         $process = $pro_uid == '' ? array ('not_equal' => $pro_uid
302         ) : array ('equal' => $pro_uid
303         );
304         $addTab = AdditionalTables::getAll( $start, $limit, $filter, $process );
```

CVE-2020-13526 - clientSetupAjax page

The 'sort' parameter in the download page clientSetupAjax is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
POST /sysworkflow/en/neoclassic/oauth2/clientSetupAjax HTTP/1.1
Host: [IP]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 74
Origin: https://[IP]
DNT: 1
Connection: close
Referer: https://[IP]/sysworkflow/en/neoclassic/oauth2/clientSetup
Cookie: PM-
Warning=Warning%3A+Processmaker+does+not+permit+you+to+open+multiple+tabs+in+the+same+browser+session+because+of+security+restrictions.++Thi
s+page+will+be+closed.; workspaceSkin=neoclassic; PHPSESSID=fnqndjde6cctk4rtpjgp63eru7; PM-TabPrimary=101010010; pm_sys_sys={"sys_sys":
"workflow"}; singleSignOn=0

start=0&limit=20&option=LST&pageSize=20&search=&sort=CLIENT_NAME[SQL INJECTION]&dir=ASC
```

The `sort` parameter is vulnerabile to SQL Injection in `workflow/engine/methods/oauth2/clientSetupAjax.php` on line 76. The parameter eventually formulates a query which will be executed in the backend database after the `getAll` function is called.

```
 72     case "LST":
 73         $pageSize = $_POST["pageSize"];
 74         $search = $_POST["search"];
 75
 76         $sortField = (isset($_POST["sort"]))? $_POST["sort"]: "";
 77         $sortDir   = (isset($_POST["dir"]))? $_POST["dir"]: "";
 78         $start = (isset($_POST["start"]))? $_POST["start"]: 0;
 79         $limit = (isset($_POST["limit"]))? $_POST["limit"]: $pageSize;
 80
 81         try {
 82             $oclient = new OauthClients();
 83             $result = $oclient->getAll(array("USR_UID" => $_SESSION["USER_LOGGED"], "SEARCH" => $search), $sortField, $sortDir, $start,
$limit);
 84
 85             $response["status"]  = "OK";
 86             $response["success"] = true;
 87             $response["resultTotal"] = $result["numRecTotal"];
 88             $response["resultRoot"]  = $result["data"];
 89         } catch (Exception $e) {
 90             $response["status"]  = "ERROR";
 91             $response["message"] = $e->getMessage();
 92         }
 93         break;
 94 }
 95
 96 echo G::json_encode($response);
```

Timeline

2020-07-21 - Vendor Disclosure

2020-10-21 - Disclosure release deadline extended 30 days

2020-11-04 - Vendor acknowledged timeline for patch

2020-11-17 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.
