Talos Vulnerability Report

TALOS-2020-1208

OpenClinic GA web portal multiple SQL injection vulnerabilities in 'listImmoLabels.jsp' page

APRIL 13, 2021

CVE NUMBER

CVE-2020-27242, CVE-2020-27243, CVE-2020-27244, CVE-2020-27245, CVE-2020-27246

Summary

A number of exploitable SQL injection vulnerabilities exists in 'listImmoLabels.jsp' page of OpenClinic GA 5.173.3 application. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.

Tested Versions

OpenClinic GA 5.173.3

Product URLs

https://sourceforge.net/projects/open-clinic/

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

OpenClinic GA is an open source fully integrated hospital management solution.

Multiple SQL injection vulnerabilities exist in the `listImmoLabels.jsp` page of OpenClinic GA. These vulnerabilities are the result of dynamic use of parameters in prepared statements as seen in the souce code of listImmoLabels.jsp below:

```
        <%
//*** FIND ************************************************
if(sAction.equalsIgnoreCase("find")){
        String sSql = "select * from OC_IMMO where 1 = 1 ";

        if(sImmoService.length() > 0){
                sSql+= "and OC_IMMO_SERVICEUID like '"+sImmoService+"%'";
        }
        if(sImmoLocation.length() > 0){
                sSql+= "and OC_IMMO_LOCATION like '"+sImmoLocation+"%'";
        }
        if(sImmoCode.length() > 0){
                sSql+= "and OC_IMMO_CODE like '"+sImmoCode+"%'";
        }
        if(sImmoBuyer.length() > 0){
                sSql+= "and OC_IMMO_BUYER like '"+sImmoBuyer+"%'";
        }
        if(sImmoComment.length() > 0){
                sSql+= "and OC_IMMO_COMMENT like '%"+sImmoComment+"%'";
        }

        Debug.println(sSql);
        PreparedStatement ps = oc_conn.prepareStatement(sSql);
        ResultSet rs = ps.executeQuery();

        String sService, sLocation, sCode, sBuyer, sComment, sClass = "";
        int recordCount = 0;
    %>
```

The above code results in the following vulnerabilities.

CVE-2020-27242 - SQLinjection in the `immoLocation` parameter

The `immoLocation` parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/main.do?Page=util/listImmoLabels.jsp&ts=Fri%20Oct%2030%202020%2010:06:23%20GMT+0300%20(Arabian%20Standard%20Time) HTTP/1.1
Host: [...]:10080
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[...]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[...]:10080/openclinic/main.do?Page=util/listImmoLabels.jsp&ts=1603993476003
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=64BC25CBE4CE5E171D2A859C058194BA
Connection: close

Action=find&serverId=&objectId=&immoService=&immoServiceName=&immoLocation=asd<SQLINJECTION>&immoCode=asd&immoBuyer=asd&immoComment=asd
```

CVE-2020-27243 - SQLinjection in the `immoService` parameter

The `immoService` parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/main.do?
Page=util/listImmoLabels.jsp&ts=Fri%20Oct%2030%202020%2010:06:23%20GMT+0300%20(Arabian%20Standard%20Time) HTTP/1.1
Host: [...]:10080
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[...]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[...]:10080/openclinic/main.do?Page=util/listImmoLabels.jsp&ts=1603993476003
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=64BC25CBE4CE5E171D2A859C058194BA
Connection: close

Action=find&serverId=&objectId=&immoService=<SQLINJECTION>&immoServiceName=&immoLocation=asd&immoCode=asd&immoBuyer=asd&immoComment=asd
```

CVE-2020-27244 - SQLinjection in the `immoCode` parameter

The `immoCode` parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/main.do?Page=util/listImmoLabels.jsp&ts=Fri%20Oct%2030%202020%2010:06:23%20GMT+0300%20(Arabian%20Standard%20Time) HTTP/1.1
Host: [...]:10080
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[...]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[...]:10080/openclinic/main.do?Page=util/listImmoLabels.jsp&ts=1603993476003
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=64BC25CBE4CE5E171D2A859C058194BA
Connection: close

Action=find&serverId=&objectId=&immoService=&immoServiceName=&immoLocation=asd&immoCode=asd<SQLINJECTION>&immoBuyer=asd&immoComment=asd
```

CVE-2020-27245 - SQLinjection in the `immoBuyer` parameter

The `immoBuyer` parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/main.do?Page=util/listImmoLabels.jsp&ts=Fri%20Oct%2030%202020%2010:06:23%20GMT+0300%20(Arabian%20Standard%20Time) HTTP/1.1
Host: [...]:10080
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[...]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[...]:10080/openclinic/main.do?Page=util/listImmoLabels.jsp&ts=1603993476003
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=64BC25CBE4CE5E171D2A859C058194BA
Connection: close

Action=find&serverId=&objectId=&immoService=&immoServiceName=&immoLocation=asd&immoCode=asd&immoBuyer=asd<SQLINJECTION>&immoComment=asd
```

CVE-2020-27246 - SQLinjection in the `immoComment` parameter

The `immoComment` parameter in the 'listImmoLabels.jsp' page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/main.do?Page=util/listImmoLabels.jsp&ts=Fri%20Oct%2030%202020%2010:06:23%20GMT+0300%20(Arabian%20Standard%20Time) HTTP/1.1
Host: [...]:10080
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[...]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[...]:10080/openclinic/main.do?Page=util/listImmoLabels.jsp&ts=1603993476003
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: JSESSIONID=64BC25CBE4CE5E171D2A859C058194BA
Connection: close

Action=find&serverId=&objectId=&immoService=&immoServiceName=&immoLocation=asd&immoCode=asd&immoBuyer=asd&immoComment=asd<SQLINJECTION>
```

Timeline

2020-11-19 - Initial contact

2020-12-07 - 2nd contact; copy of advisories issued and vendor acknowledged receipt

2021-02-01 - 60 day follow up; no response

2021-03-09 - 90 day follow up; no response

2021-03-22 - Final notice

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.