Talos Vulnerability Report

TALOS-2020-1205

OpenClinic GA web portal multiple SQL injection vulnerabilities in 'patientslist.do' page

APRIL 13, 2021

CVE NUMBER

CVE-2020-27229, CVE-2020-27230, CVE-2020-27231

Summary

A number of exploitable SQL injection vulnerabilities exists in ‘patientslist.do’ 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 authenticated SQL injection vulnerabilities exist in the `patientslist.do` page in the parameters `findPersonID`, `findSector` and `findDistrict`. The vulnerablities occur in the same Java class after the JSP source file invokes the following function in “patientslist.jsp” :

```
 [...]
    else{
       if((simmatnew+sArchiveFileCode+snatreg+sName+sFirstname+sDateOfBirth+sPersonID+sDistrict+sSector).length()>0){
               //sDateOfBirth = ScreenHelper.convertToEUDate(sDateOfBirth); // to match with EU-date in database
               lResults =
AdminPerson.getAllPatients(simmatnew,sArchiveFileCode,snatreg,sName,sFirstname,sDateOfBirth,sPersonID,sDistrict,iMaxResultSet,sSector)   ;
        }
        else {
               lResults = new ArrayList();
 [...]
```

Above code will eventually lead to the following function which constructs final SQL query in net.admin.AdminPerson.java source file between lines 2500 and 2627:

[...]

```
public static List getAllPatients(String simmatnew, String sArchiveFileCode, String snatreg, String sName, String sFirstname, String
sDateOfBirth, String sPersonID, String sDistrict) {
PreparedStatement ps = null;
ResultSet rs = null;

List lResultList = new ArrayList();

String sSQLSelect = " SELECT DISTINCT a.searchname, a.personid, a.immatnew, a.natreg, a.lastname, a.firstname, a.gender, a.dateofbirth,
a.pension";
String sSQLFrom = " FROM AdminView a";
String sSQLWhere = " 1=1 AND";

if (simmatnew.trim().length() > 0)
{
  sSQLWhere = sSQLWhere + " immatnew like '" + simmatnew + "%' AND";
}

Connection oc_conn = MedwanQuery.getInstance().getOpenclinicConnection();

if (sArchiveFileCode.trim().length() > 0) {
  String lowerArchiverFileCode = ScreenHelper.getConfigParam("lowerCompare", "archiveFileCode", oc_conn);
  sSQLWhere = sSQLWhere + " " + lowerArchiverFileCode + " LIKE '" + sArchiveFileCode.toLowerCase() + "' AND";
}

if (snatreg.trim().length() > 0) {
  sSQLWhere = sSQLWhere + " natreg like '" + snatreg + "%' AND";
}

if (sPersonID.trim().length() > 0) {
  sSQLWhere = sSQLWhere + " a.personid = " + sPersonID + " AND";
}

if (sDistrict.trim().length() > 0) {
  sSQLFrom = sSQLFrom + ", AdminPrivate p";
  sSQLWhere = sSQLWhere + " p.personid = a.personid AND district = '" + sDistrict + "' AND";
}

sName = ScreenHelper.normalizeSpecialCharacters(sName);
sFirstname = ScreenHelper.normalizeSpecialCharacters(sFirstname);
[...]
```

CVE-2020-27229 - SQL injection in the `findPersonID` parameter

The `findPersonID` parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/patientslist.do?ts=1603967526083 HTTP/1.1
Referer: http://[IP]:10080/openclinic/main.do?ts=1603968153402
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Accept-Encoding: gzip, deflate
Content-Length: 245
Host: [IP]:10080
Cookie: JSESSIONID=C3AEAECEA33285FCCE9E02171E8B3FA1
Connection: close

RSIndex=&ListAction=&findSearchButtonClick=Find&findName=A&findFirstname=&findDateOfBirth=&findnatreg=&findimmatnew=9967&findArchiveFileCode
=&findPersonID=<SQLINJECTION>&findUnitText=&Action=&findUnit=&findDistrict=&findSector=
```

CVE-2020-27230 - SQL injection in the `findSector` parameter

The `findSector` parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/patientslist.do?ts=1603967526083 HTTP/1.1
Referer: http://[IP]:10080/openclinic/main.do?ts=1603968153402
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Accept-Encoding: gzip, deflate
Content-Length: 258
Host: [IP]:10080
Cookie: JSESSIONID=C3AEAECEA33285FCCE9E02171E8B3FA1
Connection: close

RSIndex=&ListAction=&findSearchButtonClick=Find&findName=A&findFirstname=&findDateOfBirth=&findnatreg=&findimmatnew=9967&findArchiveFileCode
=&findPersonID=9967&findUnitText=&Action=&findUnit=&findDistrict=&findSector=<SQLINJECTION>
```

CVE-2020-27231 - SQL injection in the `findDistrict` parameter

The `findDistrict` parameter in ‘‘patientslist.do’ page is vulnerable to authenticated SQL injection. The following request would trigger the vulnerability:

```
POST /openclinic/patientslist.do?ts=1603967526083 HTTP/1.1
Referer: http://[IP]:10080/openclinic/main.do?Page=_common/start.jsp&NextPage=ok&CheckEmail=true
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Accept-Encoding: gzip, deflate
Content-Length: 250
Host: [IP]:10080
Cookie: JSESSIONID=C3AEAECEA33285FCCE9E02171E8B3FA1
Connection: close

RSIndex=&ListAction=&findSearchButtonClick=Find&findName=a&findFirstname=&findDateOfBirth=&findnatreg=&findimmatnew=&findArchiveFileCode=&fi
ndPersonID=&findUnitText=&Action=&findUnit=&findDistrict=<SQLINJECTION>&findSector=
```

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.