Talos Vulnerability Report

TALOS-2020-1207

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

APRIL 13, 2021

CVE NUMBER

CVE-2020-27233, CVE-2020-27234, CVE-2020-27235, CVE-2020-27236, CVE-2020-27237, CVE-2020-27238, CVE-2020-27239, CVE-2020-27240, CVE-2020-27241

Summary

Multiple exploitable SQL injection vulnerabilities exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. 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 injections exist in the due to a lack of filtering applied in the ‘getAssets.jsp’ source file and underlying ‘be.Asset.Asset.java’ Java class when input parameters are used to create Asset object as seen below:

```
Asset findObject = new Asset();
findObject.code = sCode;
findObject.nomenclature = sNomenclatureCode;
findObject.description = sDescription;
findObject.serialnumber = sSerialnumber;
findObject.comment9 = sAssetStatus;
findObject.supplierUid = sSupplierUID;
findObject.serviceuid = sServiceUid;
findObject.comment15=sCompNomenclatureCode;
findObject.comment16=sComponentStatus;

if(sPurchasePeriodBegin.length() > 0){
    findObject.purchasePeriodBegin = ScreenHelper.parseDate(sPurchasePeriodBegin);
}

if(sPurchasePeriodEnd.length() > 0){
    findObject.purchasePeriodEnd = ScreenHelper.parseDate(sPurchasePeriodEnd);
}

List assets = Asset.getList(findObject);
String sReturn = "";
```

After above object is construct the SQL query is created and, eventually, executed as seen below:

```
 [...]
 if (findItem.code.length() > 0) {
    sSql = sSql + " AND (OC_ASSET_CODE = '" + findItem.code + "' or OC_ASSET_SERVERID||'.'||OC_ASSET_OBJECTID = '" + findItem.code + "')";
  }
  if (ScreenHelper.checkString(findItem.description).length() > 0) {
    sSql = sSql + " AND OC_ASSET_DESCRIPTION LIKE '%" + findItem.description + "%'";
  }
  if (ScreenHelper.checkString(findItem.serviceuid).length() > 0) {
    sSql = sSql + " AND OC_ASSET_SERVICE LIKE '" + findItem.serviceuid + "%'";
  }
  if (ScreenHelper.checkString(findItem.serialnumber).length() > 0) {
    sSql = sSql + " AND OC_ASSET_SERIAL LIKE '%" + findItem.serialnumber + "%'";
  }
  if (ScreenHelper.checkString(findItem.assetType).length() > 0) {
    sSql = sSql + " AND OC_ASSET_TYPE = '" + findItem.assetType + "'";
  }
  if (ScreenHelper.checkString(findItem.comment9).length() > 0) {
    sSql = sSql + " AND OC_ASSET_COMMENT9 = '" + findItem.comment9 + "'";
  }
  if (ScreenHelper.checkString(findItem.nomenclature).length() > 0) {
    sSql = sSql + " AND OC_ASSET_NOMENCLATURE LIKE '" + findItem.nomenclature + "%'";
  }
  if (ScreenHelper.checkString(findItem.nomenclature).length() > 0) {
    sSql = sSql + " AND OC_ASSET_NOMENCLATURE LIKE '" + findItem.nomenclature + "%'";
  }
  if (ScreenHelper.checkString(findItem.comment15).length() > 0) {
    sSql = sSql + " AND OC_ASSET_COMMENT15 LIKE '%" + findItem.comment15 + ";%'";
  }
  if (ScreenHelper.checkString(findItem.comment16).length() > 0) {
    sSql = sSql + " AND EXISTS (select * from OC_ASSETCOMPONENTS where OC_COMPONENT_ASSETUID=OC_ASSET_SERVERID||'.'||OC_ASSET_OBJECTID and
OC_COMPONENT_NOMENCLATURE like '" + (ScreenHelper.checkString(findItem.comment15).length() == 0 ? "%" : findItem.comment15) + "' and
OC_COMPONENT_STATUS='" + findItem.comment16 + "')";
  }
  if (ScreenHelper.checkString(findItem.supplierUid).length() > 0) {
    sSql = sSql + " AND OC_ASSET_SUPPLIERUID like '%" + findItem.supplierUid + "%'";
  }
  [...]
```

CVE-2020-27233 - SQLinjection in the `supplierUID` parameter

The `supplierUID` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?
ts=1603998759824&code=&nomenclature=&compnomenclature=y&description=&showinactive=false&serviceuid=&serialnumber=&assetStatus=&componentStat
us=&supplierUID=<SQLINJECTION>&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27234 - SQLinjection in the `serviceuid` parameter

The serviceuid parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?
ts=1603998759824&code=&nomenclature=&compnomenclature=y&description=&showinactive=false&serviceuid=
<SQLINJECTION>&serialnumber=&assetStatus=&componentStatus=&supplierUID=&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27235 - SQLinjection in the `description` parameter

The `description` parameter in `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?ts=1603998759824&code=&nomenclature=&compnomenclature=y&description=
<SQLINJECTION>&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=&componentStatus=&supplierUID=&purchasePeriodBegin=&skip=0&pu
rchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27236 - SQLinjection in the `compnomenclature` parameter

The `compnomenclature` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?ts=16039987598246code=&nomenclature=&compnomenclature=
<SQLINJECTION>y&description=&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=&componentStatus=&supplierUID=&purchasePeriodBe
gin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27237 - SQLinjection in the `nomenclature` parameter

The `nomenclature` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?ts=16039987598246code=&nomenclature=
<SQLINJECTION>&compnomenclature=&description=&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=&componentStatus=&suppplierUID=
&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27238 - SQLinjection in the `code` parameter

The `code` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?ts=16039987598246code=
<SQLINJECTION>&nomenclature=&compnomenclature=&description=&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=&compnentStatus=
&supplierUID=&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27239 - SQLinjection in the `assetStatus` parameter

The `assetStatus` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?
ts=16039987598246code=&nomenclature=&compnomenclature=&description=&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=
<SQLINJECTION>&componentStatus=&supplierUID=&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27240 - SQLinjection in the `componentStatus` parameter

The `componentStatus` parameter inthe `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?
ts=16039987598426code=&nomenclature=&compnomenclature=&description=&showinactive=false&serviceuid=cli.gen&serialnumber=&assetStatus=
<SQLINJECTION>&componentStatus=&supplierUID=&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

CVE-2020-27241 - SQLinjection in the `serialnumber` parameter

The `serialnumber` parameter in the `getAssets.jsp` page is vulnerable to unauthenticated SQL injection. The following request would trigger the vulnerability:

```
GET /openclinic/assets/ajax/asset/getAssets.jsp?
ts=1603998759824&code=&nomenclature=&compnomenclature=y&description=&showinactive=false&serviceuid=&serialnumber=
<SQLINJECTION>&assetStatus=&componentStatus=&supplierUID=&purchasePeriodBegin=&skip=0&purchasePeriodEnd= HTTP/1.1
Host: [IP]:10080
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.7.3
X-Requested-With: XMLHttpRequest
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
Referer: http://[IP]:10080/openclinic/main.do?Page=assets/manage_assets.jsp&ts=1603998735385
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

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

2021-04-13 - Final notice

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.
