Talos Vulnerability Report

TALOS-2020-1075

OS4Ed openSIS CoursePeriodModal.php page multiple SQL injection vulnerabilities

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6126, CVE-2020-6127, CVE-2020-6128

Summary

Multiple exploitable SQL injection vulnerabilities exist in the CoursePeriodModal.php page of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.

Tested Versions

OS4Ed openSIS 7.3

Product URLs

https://opensis.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

openSIS is a student information system and school management system. It is available in commercial and open-source versions. It allows schools to create schedules and track attendance, grades and transcripts.

CVE-2020-6126 - Parameter “course_period_id”

The `course_period_id` parameter in the page `CoursePeriodModal.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CoursePeriodModal.php?id=1&course_period_id=1[SQLINJECTION]&modname=1&subject_id=1&course_id=1&meet_date=1 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/opensis/Modules.php?modname=eligibility/Student.php&modfunc=add&start_date=
Cookie: miniSidebar=0; PHPSESSID=6chg16qcanbg3adrqlq6sm6fa3
Upgrade-Insecure-Requests: 1
```

The vulnerable code for this parameter is also at line 24:

```
 22     }
 23     else {
 24         $cpblocked_RET = DBGet(DBQuery("SELECT COURSE_PERIOD_DATE,PERIOD_ID,ROOM_ID,DOES_ATTENDANCE FROM course_period_var where 
course_period_id=$_REQUEST[course_period_id] AND course_period_date='" . $_REQUEST['meet_date'] . "' AND id='" . $_REQUEST['id'] . "'"));
 25         $cpblocked_RET = $cpblocked_RET[1];
 26         $periods_RET = DBGet(DBQuery("SELECT PERIOD_ID,TITLE FROM school_periods WHERE SCHOOL_ID='" . UserSchool() . "' AND SYEAR='" . 
UserSyear() . "' ORDER BY SORT_ORDER"));
 27         if (count($periods_RET)) {
 28             foreach ($periods_RET as $period)
 29                 $periods[$period['PERIOD_ID']] = $period['TITLE'];
 30         }
```

CVE-2020-6127 - Parameter “id”

The `id` parameter in the page `CoursePeriodModal.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CoursePeriodModal.php?id=1[SQLINJECTION]&course_period_id=1&modname=1&subject_id=1&course_id=1&meet_date=1 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/opensis/Modules.php?modname=eligibility/Student.php&modfunc=add&start_date=
Cookie: miniSidebar=0; PHPSESSID=6chg16qcanbg3adrqlq6sm6fa3
Upgrade-Insecure-Requests: 1
```

The vulnerable code for this parameter is at line 24:

```
 22     }
 23     else {
 24         $cpblocked_RET = DBGet(DBQuery("SELECT COURSE_PERIOD_DATE,PERIOD_ID,ROOM_ID,DOES_ATTENDANCE FROM course_period_var where
course_period_id=$_REQUEST[course_period_id] AND course_period_date='" . $_REQUEST['meet_date'] . "' AND id='" . $_REQUEST['id'] . "'"));
 25         $cpblocked_RET = $cpblocked_RET[1];
 26         $periods_RET = DBGet(DBQuery("SELECT PERIOD_ID,TITLE FROM school_periods WHERE SCHOOL_ID='" . UserSchool() . "' AND SYEAR='" .
UserSyear() . "' ORDER BY SORT_ORDER"));
 27         if (count($periods_RET)) {
 28             foreach ($periods_RET as $period)
 29                 $periods[$period['PERIOD_ID']] = $period['TITLE'];
 30         }
```

CVE-2020-6128 - Parameter “meet_date”

The `meet_date` parameter in the page `CoursePeriodModal.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CoursePeriodModal.php?id=1&course_period_id=1&modname=1&subject_id=1&course_id=1&meet_date=1[SQLINJECTION] 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/opensis/Modules.php?modname=eligibility/Student.php&modfunc=add&start_date=
Cookie: miniSidebar=0; PHPSESSID=6chg16qcanbg3adrqlq6sm6fa3
Upgrade-Insecure-Requests: 1
```

The vulnerable code for this parameter is also at line 24:

```
 22     }
 23     else {
 24         $cpblocked_RET = DBGet(DBQuery("SELECT COURSE_PERIOD_DATE,PERIOD_ID,ROOM_ID,DOES_ATTENDANCE FROM course_period_var where
course_period_id=$_REQUEST[course_period_id] AND course_period_date='" . $_REQUEST['meet_date'] . "' AND id='" . $_REQUEST['id'] . "'"));
 25         $cpblocked_RET = $cpblocked_RET[1];
 26         $periods_RET = DBGet(DBQuery("SELECT PERIOD_ID,TITLE FROM school_periods WHERE SCHOOL_ID='" . UserSchool() . "' AND SYEAR='" .
UserSyear() . "' ORDER BY SORT_ORDER"));
 27         if (count($periods_RET)) {
 28             foreach ($periods_RET as $period)
 29                 $periods[$period['PERIOD_ID']] = $period['TITLE'];
 30         }
```

Timeline

2020-06-02 - Vendor Disclosure

2020-08-13 - Vendor provided patch to Talos for testing

2020-08-17 - Talos confirmed patch resolved issue

2020-08-31 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1074

NEXT REPORT

TALOS-2020-1076