Talos Vulnerability Report

TALOS-2020-1072

OS4Ed openSIS CheckDuplicateStudent.php page SQL injection vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6117,CVE-2020-6119,CVE-2020-6121,CVE-2020-6118,CVE-2020-6120,CVE-2020-6122

SUMMARY

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

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

OS4Ed openSIS 7.3

PRODUCT URLS

openSIS - 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.

The following code in CheckDuplicateStudent is vulnerable to multiple SQL injection attacks at lines 64 and 66:

```
 31         $student_fname= $_REQUEST['fn'];
 32         $student_mname = $_REQUEST['mn'];
 33         $student_lname = $_REQUEST['ln'];
 34         $student_byear = $_REQUEST['byear'];
 35         $student_bmonth = $_REQUEST['bmonth'];
 36         $student_bday = $_REQUEST['bday'];
 37
 [...]
 62    $student_birthday =trim($student_byear).'-'.  trim($student_bmonth).'-'.  trim($student_bday);
 63 if(trim($student_mname)=='')
 64 $chechk_stu = 'SELECT s.student_id AS ID FROM students s,student_enrollment se WHERE s.student_id=se.student_id AND
lcase(s.last_name)="'.strtolower($student_lname).'" AND lcase(s.first_name)="'.strtolower($student_fname).'" AND (lcase(s.middle_name)="" OR
lcase(s.middle_name) IS NULL ) AND s.birthdate="'.$student_birthday.'"  AND se.syear="'.$_SESSION['UserSyear'].'" AND
se.school_id="'.$_SESSION['UserSchool'].'    " ';
 65 else
 66 $chechk_stu = 'SELECT s.student_id AS ID FROM students s,student_enrollment se WHERE s.student_id=se.student_id AND
lcase(s.last_name)="'.strtolower($student_lname).'" AND lcase(s.first_name)="'.strtolower($s    tudent_fname).'" AND
lcase(s.middle_name)="'.strtolower($student_mname).'" AND s.birthdate="'.$student_birthday.'"  AND se.syear="'.$_SESSION['UserSyear'].'" AND
se.school_id="'.$_SESSION['UserSchool'].'"  ';
 67 $chechk_stu_result = DBGet(DBQuery($chechk_stu));
 68 $prev_student = count($chechk_stu_result);
 69   echo $prev_student;
```

The following sections detail the specific parameters and how they can be exploited.

CVE-2020-6117 - Parameter "bday"

The `bday` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1&mn=1&ln=1&byear=1&bmonth=1&bday=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
```

CVE-2020-6118 - Parameter “bmonth”

The `bmonth` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1&mn=1&ln=1&byear=1&bmonth=1[SQLINJECTION]&bday=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
```

CVE-2020-6119 - Parameter “byear”

The `byear` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1&mn=1&ln=1&byear=1[SQLINJECTION]&bmonth=1&bday=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
```

CVE-2020-6120 - Parameter “fn”

The `fn` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1[SQLINJECTION]&mn=1&ln=1&byear=1&bmonth=1&bday=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
```

CVE-2020-6121 - Parameter “ln”

The `ln` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1&mn=1&ln=1[SQLINJECTION]&byear=1&bmonth=1&bday=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
```

CVE-2020-6122 - Parameter “mn"

The `mn` parameter in the page `CheckDuplicateStudent.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/CheckDuplicateStudent.php?fn=1&mn=1[SQLINJECTION]&ln=1&byear=1&bmonth=1&bday=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
```

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.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.