Talos Vulnerability Report

TALOS-2020-1074

OS4Ed openSIS GetSchool.php SQL injection Vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6125

Summary

An exploitable SQL injection vulnerability exists in the GetSchool.php functionality 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 this vulnerability.

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.

The `u` parameter in the page `GetSchool.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/GetSchool.php?title=1&course_period_id=1&u=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 at line 32:

```
 31                $marking_period = $_GET['u'];
 32                $get_schoolname = DBGet(DBQuery("SELECT school_name FROM  history_marking_periods  WHERE marking_period_id =
$marking_period"));
 33         if($get_schoolname[1]['school_name'])
 34             echo $get_schoolname[1]['school_name'];
 35         else
 36         {
 37              $get_schoolid = DBGet(DBQuery("SELECT school_id FROM  marking_periods  WHERE marking_period_id = $marking_period"));
 38              if($get_schoolid[1]['school_id'])
 39              {
 40                 $get_schoolid = DBGet(DBQuery("SELECT title FROM  schools  WHERE id = $get_schoolid[1][school_id]"));
 41                  echo $get_schoolid[1]['title'];
 42              }
 43         }
```

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.