Talos Vulnerability Report

TALOS-2020-1078

OS4Ed openSIS Validator.php SQL injection vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6135

Summary

An exploitable SQL injection vulnerability exists in the Validator.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 `stfid` parameter in the page `Validator.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/Validator.php?u=1234566stfid=1[SQLINJECTION]&password=1&validate=pass 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: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://[IP]/opensis/Modules.php?modname=schoolsetup/Schools.php&modfunc=update
Cookie: miniSidebar=0; PHPSESSID=6chg16qcanbg3adrqlq6sm6fa3
```

The vulnerable code for this parameter is at line 41:

```
 30         include 'Warehouse.php';
 31                         $flag = $_GET['u'];
 32           $usr = substr($flag, -4);
 33
 34         // ------------------------ For Unique Checking ---------------------------------- //
 35         $un = substr($flag, 0, -4);
 36         $un = strtoupper($un);
 37         // ------------------------ For Unique Checking ---------------------------------- //
 38          switch ($_GET['validate'])
 39         {
 40             case 'pass':
 41                         $res_pass_chk = DBQuery("SELECT * FROM login_authentication WHERE password = '".md5($_GET['password'])."' AND
user_id!='".$_GET['stfid']."' AND profile_id=0");
 42                         $num_pass = $res_pass_chk->num_rows;
 43                         if($num_pass==0)
 44                         {
 45                             echo 1;
 46
 47                         }
 48                 break;
 49
```

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.