Talos Vulnerability Report

TALOS-2020-1079

OS4Ed openSIS DownloadWindow.php SQL injection vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6136

Summary

An exploitable SQL injection vulnerability exists in the DownloadWindow.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 `down_id` parameter in the download page `DownloadWindow.php` is vulnerable to SQL injection.

Below is an example request that will trigger the vulnerability:

```
GET /opensis/DownloadWindow.php?down_id=1[SQLINJECTION]&filename=1&name=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: */*
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 33:

```
 28 include('RedirectRootInc.php');
 29 include 'Warehouse.php';
 30 include 'Data.php';
 31 if(isset($_REQUEST['down_id']) && $_REQUEST['down_id']!='')
 32 {
 33     $downfile_info= DBGet(DBQuery('SELECT * FROM user_file_upload WHERE ID='.$_REQUEST['down_id'].''));
 34         header("Cache-Control: public");
 35         header("Pragma: ");
 36         header("Expires: 0");
 37         header("Cache-Control: must-revalidate, post-check=0, pre-check=0");
 38         header("Cache-Control: private",false); // required for certain browse
```

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-2020-1078

NEXT REPORT

TALOS-2020-1080