Talos Vulnerability Report

TALOS-2020-1081

OS4Ed openSIS login SQL injection vulnerability

AUGUST 31, 2020

CVE NUMBER

CVE-2020-6141

Summary

An exploitable SQL injection vulnerability exists in the login functionality of OS4Ed openSIS 7.3. A specially crafted HTTP request can lead to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

OS4Ed openSIS 7.3

Product URLs

https://opensis.com/

CVSSv3 Score

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

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 parameters are vulnerable to unauthenticated SQL injection attacks:

`USERNAME` parameter in `/opensis/index.php`:

```
POST /opensis/index.php 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: 30
Origin: http://[IP]
DNT: 1
Connection: close
Referer: http://[IP]/opensis/index.php?modfunc=logout&ins=comp
Upgrade-Insecure-Requests: 1

USERNAME=123[SQL INJECTION]&PASSWORD=123&log=
```

The vulnerable code for `opensis/index.php` is at line 117 is due to a lack of input sanitation leading:

```
99     $username = optional_param('USERNAME', '', PARAM_RAW);
100     if($_REQUEST['remember'])
101       {
102       $cName='remember_me_name';
103       $cPwd='remember_me_pwd';
104       setcookie($cName, $username, time()+60*60*24*100, "/");
105       setcookie($cPwd, optional_param('PASSWORD','',PARAM_RAW), time()+60*60*24*100, "/");
106       }
107       else
108       {
109       setcookie('remember_me_name', 'gone', time()-60*60*24*100, "/");
110       setcookie('remember_me_pwd', 'gone', time()-60*60*24*100, "/");
111       }
112     if ($password == optional_param('PASSWORD', '', PARAM_RAW))
113         $password = str_replace("\'", "", md5(optional_param('PASSWORD', '', PARAM_RAW)));
114     $password = str_replace("&", "", md5(optional_param('PASSWORD', '', PARAM_RAW)));
115     $password = str_replace("\\", "", md5(optional_param('PASSWORD', '', PARAM_RAW)));
116
117     $login_uniform = DBGet(DBQuery('SELECT * FROM login_authentication WHERE UPPER(USERNAME)=UPPER(\'' . $username . '\') AND
UPPER(PASSWORD)=UPPER(\'' . $password . '\')'));
118
```

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-2020-1036

NEXT REPORT TALOS-2020-1083
