

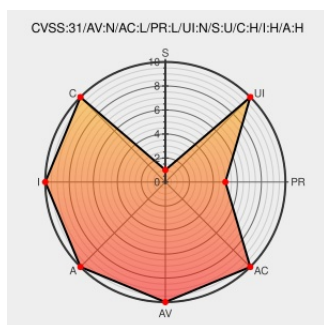


CVE-2021-40309

Published on: 09/24/2021 12:00:00 AM UTC

Last Modified on: 10/01/2021 02:03:00 AM UTC

CVE-2021-40309

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Opensis](#) from [Os4ed](#) contain the following vulnerability:

A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. allows an attacker to inject their own SQL query. The cp_id_miss_attn parameter from TakeAttendance.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request as a user with access to "Take Attendance" functionality to trigger this vulnerability.

CVE-2021-40309 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
OpenSIS Community 8.0 - 'cp_id_miss_attn' SQL Injection - PHP webapps Exploit	www.exploit-db.com Proof of Concept	MISC www.exploit-db.com/exploits/50249

[text/html](#)

GitHub - OS4ED/openSIS-Classic: openSIS is a commercial grade, secure, scalable & intuitive Student Information System, School Management Software from OS4ED. Has all functionalities to run single or multiple institutions in one installation. Web based, php code, MySQL database.

[github.com](#)[text/html](#)

 MISC github.com/OS4ED/openSIS-Classic

Vulnerability-Reports-and-Disclosures/OpenSIS-Community-8.0.md at main · MiSERYYYYY/Vulnerability-Reports-and-Disclosures · GitHub

[github.com](#)[text/html](#)

 MISC github.com/MiSERYYYYY/Vulnerability-Reports-and-Disclosures/blob/main/OpenSIS-Community-8.0.md

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Os4ed	Opensis	8.0	All	All	All
cpe:2.3:a:os4ed:opensis:8.0:*:*:*:community:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-40309 : A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0.... twitter.com/i/web/status/1...	2021-09-24 16:05:50
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-40309 Description: CVE-2021-40309 A SQL injection vulnerability exists... twitter.com/i/web/status/1...	2021-09-24 17:00:05
 @0_exploit	CVE-2021-40309 dlvr.it/S8GS9H	2021-09-24 19:51:03
 @SecRiskRptSME	RT: CVE-2021-40309 A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.... twitter.com/i/web/status/1...	2021-09-25 07:33:20
 @threatmeter	CVE-2021-40309 A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. al... twitter.com/i/web/status/1...	2021-09-26 07:09:38

[← Previous ID](#)[Next ID→](#)

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)