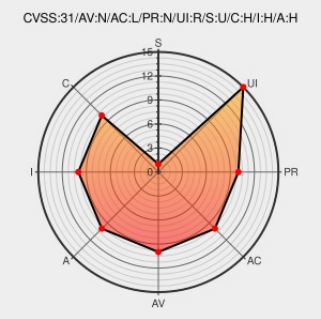
# CVE-2021-37381

Published on: 08/06/2021 12:00:00 AM UTC

Last Modified on: 08/13/2021 06:42:00 PM UTC

## CVE-2021-37381

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Graduate Management Information System from Southsoft contain the following vulnerability:

Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF. For example: any student's photo information can be accessed through /gmis/(S([1]))/student/grgl/PotoImageShow/?bh=[2]. Among them, the code in [1] is a random string generated according to the user's login related information. It can protect the user's identity, but it can not effectively prevent unauthorized access. The code in [2] is the student number of any student. The attacker can carry out CSRF attack on the system by modifying [2] without modifying [1].

CVE-2021-37381 has been assigned by 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 | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 6.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| poc_information/southsoft_GMIS.txt at main · caiteli/poc_information · GitHub | github.com text/html | MISC github.com/caiteli/poc_information/blob/main/southsoft_GMIS.txt |
| letter of thanks · Issue #1 · caiteli/poc_information · GitHub | github.com text/html | MISC github.com/caiteli/poc_information/issues/1 |

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 | Southsoft | Graduate Management Information System | 5.0 | All | All | All |

cpe:2.3:a:southsoft:graduate_management_information_system:5.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-37381 : Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private inform… twitter.com/i/web/status/1… | 2021-08-06 13:03:15 |
| @threatmeter | CVE-2021-37381 Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private informat… twitter.com/i/web/status/1… | 2021-08-07 07:14:00 |

← Previous ID

Next ID→



**CVE.report and Source URL Uptime Status status.cve.report**