VDB-355284 · CVE-2026-5531 · GCVE-100-355284

SOURCECODESTER STUDENT RESULT MANAGEMENT SYSTEM 1.0 HTTP GET REQUEST /LOGIN_CREDENTIALS.TXT CLEARTEXT STORAGE IN FILE

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.7	$0-$5k	3.09

Summary

A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been declared as problematic. The affected element is an unknown function of the file */login_credentials.txt* of the component *HTTP GET Request Handler*. The manipulation results in cleartext storage in file. This vulnerability is cataloged as CVE-2026-5531. The attack may be launched remotely. Furthermore, there is an exploit available. Applying restrictive firewalling is recommended.

Details

A vulnerability classified as problematic has been found in SourceCodester Student Result Management System 1.0. Affected is some unknown processing of the file */login_credentials.txt* of the component *HTTP GET Request Handler*. The manipulation with an unknown input leads to a cleartext storage in file vulnerability. CWE is classifying the issue as CWE-313. The product stores sensitive information in cleartext in a file, or on disk. This is going to have an impact on confidentiality.

The advisory is shared for download at drive.google.com. This vulnerability is traded as CVE-2026-5531. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1555.

The exploit is shared for download at drive.google.com. It is declared as proof-of-concept. By approaching the search of inurl:login_credentials.txt it is possible to find vulnerable targets with Google Hacking.

It is possible to mitigate the weakness by firewalling .

Product

Vendor

- SourceCodester

Name

- Student Result Management System

Version

- 1.0

License

- free

Website

- Vendor: https://www.sourcecodester.com/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.7

VulDB Base Score: 5.3
VulDB Temp Score: 4.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Cleartext storage in file
CWE: CWE-313 / CWE-312 / CWE-310
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Google Hack: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Firewall
Status: 🔍

0-Day Time: 🔒

Timeline

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Vendor: sourcecodester.com

Advisory: drive.google.com
Status: Not defined

CVE: CVE-2026-5531 (🔒)
GCVE (CVE): GCVE-0-2026-5531
GCVE (VulDB): GCVE-100-355284
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/04/2026 08:36 AM
Changes: 04/04/2026 08:36 AM (56)
Complete: 🔍
Submitter: Humraaz21
Cache ID: 52:79B:179

Submit

Accepted

- Submit #782157: SourceCodester Student Result Management System 1.0 Cleartext Storage of Sensitive Information (by Humraaz21)

Discussion

No comments yet. Languages: en.

Please log in to comment.