VDB-355435 · CVE-2026-5647 · EUVD-2026-19225

CODE-PROJECTS ONLINE SHOE STORE 1.0 ADD PRODUCT PAGE /ADMIN/ADMIN_FEATURE.PHP PRODUCT_NAME CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
2.2	$0-$5k	2.80-

Summary

A vulnerability has been found in code-projects Online Shoe Store 1.0 and classified as problematic. This vulnerability affects unknown code of the file */admin/admin_feature.php* of the component *Add Product Page*. This manipulation of the argument *product_name* causes cross site scripting. This vulnerability is registered as CVE-2026-5647. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability was found in code-projects Online Shoe Store 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown part of the file */admin/admin_feature.php* of the component *Add Product Page*. The manipulation of the argument `product_name` with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. As an impact it is known to affect integrity.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5647. The exploitation appears to be easy. The attack can be launched remotely. The exploitation requires an enhanced level of successful authentication. It demands that the victim is doing some kind of user interaction. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. By approaching the search of inurl:admin/admin_feature.php it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-19225). Similar entries are available at VDB-313305 and VDB-330124.

Product

Type

- Project Management Software

Vendor

- code-projects

Name

- Online Shoe Store

Version

- 1.0

License

- free

Website

- Vendor: https://code-projects.org/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 2.4
VulDB Meta Temp Score: 2.2

VulDB Base Score: 2.4
VulDB Temp Score: 2.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / CWE-74
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: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/06/2026	+1 days	VulDB entry last update

Sources

Vendor: code-projects.org

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5647 (🔒)
GCVE (CVE): GCVE-0-2026-5647
GCVE (VulDB): GCVE-100-355435
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 10:47 PM
Updated: 04/06/2026 02:34 PM
Changes: 04/05/2026 10:47 PM (57), 04/06/2026 02:34 PM (1)
Complete: 🔍
Submitter: Jacky_159
Cache ID: 172:F68:179

Submit

Accepted

- Submit #786171: code-projects Online Shoe Store V1.0 cross site scripting (by Jacky_159)

Discussion

No comments yet. Languages: en.

Please log in to comment.