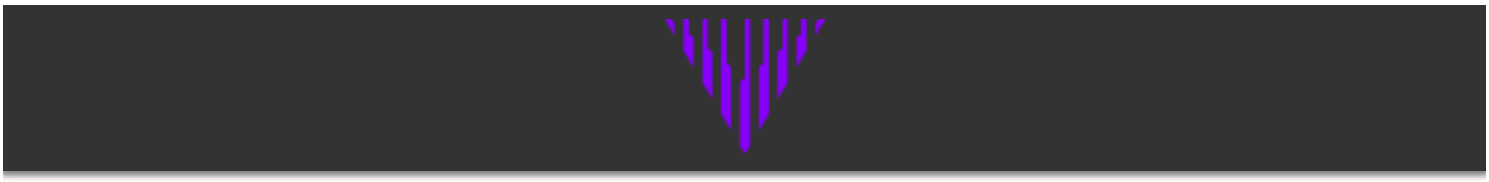

VDB-355331 · CVE-2026-5561 · GCVE-100-355331

# CAMPCODES COMPLETE POS MANAGEMENT AND INVENTORY SYSTEM UP TO 4.0.6 ENVIRONMENT VARIABLE SETTINGSCONTROLLER.PHP INJECTION

## Summary

A vulnerability marked as critical has been reported in Campcodes Complete POS Management and Inventory System up to 4.0.6. This impacts an unknown function of the file *app/Http/Controllers/SettingsController.php* of the component *Environment Variable Handler*. The manipulation leads to injection. This vulnerability is documented as CVE-2026-5561. The attack can be initiated remotely. Additionally, an exploit exists.

## Details

A vulnerability, which was classified as critical, has been found in Campcodes Complete POS Management and Inventory System up to 4.0.6. This issue affects an unknown code of the file *app/Http/Controllers/SettingsController.php* of the component *Environment Variable Handler*. The manipulation with an unknown input leads to a injection vulnerability. Using CWE to declare the problem leads to CWE-74. The product constructs all or part of a command, data structure, or record using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify how it is parsed or interpreted when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-5561. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1055 according to MITRE ATT&CK.

The exploit is available at github.com. It is declared as proof-of-concept. By approaching the search of inurl:app/Http/Controllers/SettingsController.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.

Entries connected to this vulnerability are available at VDB-352180, VDB-353253, VDB-353314 and VDB-353438.

## Product

### Vendor

- Campcodes

### Name

- Complete POS Management and Inventory System

### Version

- 4.0.0
- 4.0.1
- 4.0.2
- 4.0.3
- 4.0.4
- 4.0.5
- 4.0.6

### License

- free

### Website

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

## CPE 2.3

- 🔒
- 🔒
- 🔒

## CPE 2.2

- 🔒
- 🔒
- 🔒

## CVSSv4

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv3

**VulDB Meta Base Score**: 6.3
**VulDB Meta Temp Score**: 5.7

**VulDB Base Score**: 6.3
**VulDB Temp Score**: 5.7
**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv2



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

## Exploiting

**Class**: Injection
**CWE**: CWE-74 / CWE-707 / CWE-20
**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

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

## Sources

**Vendor**: campcodes.com

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-5561 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5561
**GCVE (VulDB)**: GCVE-100-355331
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 04/04/2026 04:09 PM
**Changes**: 04/04/2026 04:09 PM (55)
**Complete**: 🔍
**Submitter**: chenkh
**Cache ID**: 172:C64:179

## Submit

### Accepted

- Submit #782934: CampCodes Administrator Complete POS Management And Inventory System v4.0.6 remote (by chenkh)

## Discussion

No comments yet. Languages: en.

Please log in to comment.