



CodeAstro Real Estate Management System feature.php cross site scripting

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-9940
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 10:42:38 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was detected in CodeAstro Real Estate Management System 1.0. This affects an unknown function of the file

Risk And Classification

Primary CVSS: v4.0 2 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-79 | CWE-94 | CWE-79 Cross Site Scripting | CWE-94 Code Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/L/I:L/A:N
3.1	cna@vuldb.com	Secondary	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R
3.0	CNA	DECLARED	3.5	LOW	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	4		AV:N/AC:L/Au:S/C:N/I:P/A:N
2.0	CNA	DECLARED	4		AV:N/AC:L/Au:S/C:N/I:P/A:N/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codeastro	Real Estate Management System	1.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CodeAstro	Real Estate Management System	affected 1.0	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Req
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis
codeastro.com	cna@vuldb.com	codeastro.com	Product
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis
github.com/YZS17/CVE/blob/main/CodeAstro_Real_Estate_Management_System/f...	cna@vuldb.com	github.com	Exploit, Third Par
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

CNA: f10w3r (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-09-03T00:00:00.000Z	Advisory disclosed
CNA	2025-09-03T02:00:00.000Z	VulDB entry created
CNA	2025-09-03T13:55:25.000Z	VulDB entry last update

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API [cve.report/api](#)

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