



Maccms10 Database.php rep sql injection

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2025-10122
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-09 03:15:31 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was found in Maccms10 2025.1000.4050. Affected is the function rep of the file application/admin/controller/

Risk And Classification

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

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/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-74 | CWE-89 | CWE-89 SQL Injection | CWE-74 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:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	4.7	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P
2.0	CNA	DECLARED	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/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



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

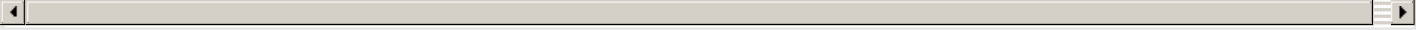
Integrity

High

Availability

High

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



CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Maccms	Maccms	10.0	2025.1000.4050	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	Maccms10	affected 2025.1000.4050	Not specified		
References						
Reference			Source	Link	Tags	
vuldb.com			cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry	
vuldb.com			cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry	
github.com/August829/Yu/blob/main/58ead8e7e08bfb016.md			cna@vuldb.com	github.com	Broken Link	
vuldb.com			cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry	
CVE Program record			CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail			NVD	nvd.nist.gov	canonical, analysis	
Vendor Comments And Credit						
Discovery Credit						
CNA: Yu Bao (VulDB User) (en)						
Additional Advisory Data						
Source	Time			Event		
CNA	2025-09-08T00:00:00.000Z			Advisory disclosed		

CNA	2025-09-08T02:00:00.000Z	VulDB entry created
CNA	2025-09-08T17:22:21.000Z	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](#)