



# baserCMS: SQL injection vulnerability in blog post

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

## Summary

<b>CVE</b>	CVE-2026-27697
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 01:16:35 UTC
<b>Updated</b>	2026-04-01 20:29:10 UTC
<b>Description</b>	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has a SQL injection vulnerability in blog

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from security-advisories@github.com

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

**EPSS:** 0.000290000 probability, percentile 0.080050000 (date 2026-04-01)

**Problem Types:** CWE-89 | CWE-89 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality  
None

Integrity  
Low

Availability  
Low

Sub Conf.  
None

Sub Integrity  
None

Sub Availability  
None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/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  
None

User Interaction  
None

Scope  
Unchanged

Confidentiality  
High

Integrity  
High

Availability  
High

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

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Basercms	Basercms	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Baserproject	Basercms	affected < 5.2.3	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/baserproject/basercms/releases/tag/5.2.3">github.com/baserproject/basercms/releases/tag/5.2.3</a>	security-advisories@github.com	<a href="https://github.com">github.com</a>	Release Note
<a href="https://github.com/baserproject/basercms/security/advisories/GHSA-vh89-rjph-2g7p">github.com/baserproject/basercms/security/advisories/GHSA-vh89-rjph-2g7p</a>	security-advisories@github.com	<a href="https://github.com">github.com</a>	Vendor Advisory
<a href="https://basercms.net/security/JVN_20837860">basercms.net/security/JVN_20837860</a>	security-advisories@github.com	<a href="https://basercms.net">basercms.net</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, cve

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)