



# SQL injection in Umami Software application

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

## Summary

<b>CVE</b>	CVE-2026-4317
<b>State</b>	PUBLISHED
<b>Assigner</b>	INCIBE
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 10:16:19 UTC
<b>Updated</b>	2026-04-01 14:24:02 UTC
<b>Description</b>	SQL injection (SQLi) vulnerability in Umami Software web application through an improperly sanitized parameter, which co

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from cve-coordination@incibe.es

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

**EPSS:** 0.000520000 probability, percentile 0.163200000 (date 2026-04-07)

**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	cve-coordination@incibe.es	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/S

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Umami Software Application</a>	Umami Software	affected 3.0.2 custom	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.incibe.es/en/incibe-cert/notices/aviso/sql-inyection-umami-software-app...">www.incibe.es/en/incibe-cert/notices/aviso/sql-inyection-umami-software-app...</a>	cve-coordination@incibe.es	<a href="http://www.incibe.es">www.incibe.es</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Hector Ruiz Ruiz & NaxusAI (en)

### Additional Advisory Data

#### Solutions

**CNA:** The vulnerability has been fixed by Umami Software team in version 3.0.3.

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

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](https://cve.report/api)

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