



CVE-2008-0519

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

Summary

CVE	CVE-2008-0519
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-31 20:00:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	SQL injection vulnerability in index.php in the Atapin Jokes (com_jokes) 1.0 component for Mambo and Joomla! allows rem

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-89 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Com Jokes	1.0	All	All	All

Application	Mambo	Com Jokes	1.0	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference	Source		Link			
Joomla! com_jokes Component 'cat' Parameter SQL Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com/bid/26611			
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www.vupen.com			
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108		exchange.xforce.ibmcloud.com/vulnerabilities/26611			
Mambo Component jokes 1.0 (cat) SQL Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.exploit-db.com/exploits/26611/			
CVE Program record	CVE.ORG		www.cve.org			
NVD vulnerability detail	NVD		nvd.nist.gov			
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						

© CVE.report 2026 |

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](#).

CVE.report and Source URL Uptime Status status.cve.report