CVE-2008-2047

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

Summary

CVE	CVE-2008-2047
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-01 19:05:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple SQL injection vulnerabilities in Angelo-Emlak 1.0 allow remote attackers to execute arbitrary SQL commands via th

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	Aspindir	Angelo-emlak	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	Lin
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	ww
Angelo-Emlak 1.0 Multiple Remote SQL injection Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	ww
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exc
angelo-emlak Cross-Site Scripting and SQL Injection Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	sec
Angelo-Emlak Multiple SQL Injection and Cross-Site Scripting Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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