CVE-2009-3802

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

Summary

CVE	CVE-2009-3802
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-27 16:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Amiro.CMS 5.4.0.0 and earlier allows remote attackers to obtain sensitive information via an invalid loginname ("%%%") to

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amirocms	Amiro.cms	4.0.8.0	All	All	All

Application	Amirocms	Amiro.cms	4.2.0.5	All	All	All
Application	Amirocms	Amiro.cms	4.2.1.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.2.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.3.0	All	All	All
Application	Amirocms	Amiro.cms	4.2.4	All	All	All
Application	Amirocms	Amiro.cms	4.2.5	All	All	All
Application	Amirocms	Amiro.cms	5.0.7	All	All	All
Application	Amirocms	Amiro.cms	5.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.2	All	All	All
Application	Amirocms	Amiro.cms	5.2.3	All	All	All
Application	Amirocms	Amiro.cms	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
IBM X-Force Exchange
ONsec.ru тесты на проникновение, исследование безопасности, устранение последствий, аудит информационной безопасности, защ
Files ≈ Packet Storm
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Amiro.CMS Cross-Site Scripting and Information Disclosure Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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