



CVE-2011-5235

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

Summary

CVE	CVE-2011-5235
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-25 17:55:08 UTC
Updated	2026-04-29 01:13:23 UTC
Description	SQL injection vulnerability in mnoGoSearch before 3.3.12 allows remote attackers to execute arbitrary SQL commands via

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	Mnogosearch	Mnogosearch	3.1.19	All	All	All

Application	Mnogosearch	Mnogosearch	3.1.20	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.10	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.13	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.14	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.15	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.16	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.17	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.18	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.19	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.20	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.21	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.22	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.23	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.24	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.25	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.26	All	All	All
Application	Mnogosearch	Mnogosearch	3.2.42	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.0	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.1	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.10	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.2	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.3	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.4	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.5	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.6	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.7	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.8	All	All	All
Application	Mnogosearch	Mnogosearch	3.3.9	All	All	All
Application	Mnogosearch	Mnogosearch	All	All	All	All

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

References						
Reference	Source					
www.mnogosearch.org/doc22/mnogosearch_channels.html	c6954c2a-0107-420b-0100-064da2661109					

www.mnogosearch.org/doc33/msearch-changeelog.html	af854a3a-2127-422b-91ae-364da2661108
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108
Security Advisory SA47272 - mnoGoSearch Hostnames SQL Injection Vulnerability - Secunia	af854a3a-2127-422b-91ae-364da2661108
mnoGoSearch Unspecified SQL Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108
www.osvdb.org/77949	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#) 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

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