



CVE-2005-3816

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

Summary

CVE	CVE-2005-3816
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-11-26 02:03:00 UTC
Updated	2011-03-08 02:27:00 UTC
Description	Multiple SQL injection vulnerabilities in forum.php in freeForum 1.1 and earlier and earlier allow remote attackers to execute

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoneo-soft	Freeforum	All	All	All	All

References

Reference	Source
Secunia - Advisories - freeForum "thread" SQL Injection Vulnerability	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
FreeForum Multiple SQL Injection Vulnerabilities	BID
- UNSECURED SYSTEMS -: freeForum 1.x "cat" and "thread" SQL inj.	MISC
SecurityTracker.com Archives - freeForum Input Validation Flaw in 'cat' and 'thread' Parameters Permits SQL Injection Attacks	SECTRAK
21086	OSVDB
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](#)