



CVE-2005-0617

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

Summary

CVE	CVE-2005-0617
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2016-10-18 03:13:00 UTC
Description	SQL injection vulnerability in dl-search.php in PostNuke 0.750 and 0.760-RC2 allows remote attackers to execute arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postnuke Software Foundation	Postnuke	0.750	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc2	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.750	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.760_rc2	All	All	All

References

Reference
403 Forbidden
'[SECURITYREASON.COM] PostNuke SQL Injection 0.760-RC2=>x cXlb8O3.3' - MARC
SecurityTracker.com Archives - PostNuke Input Validation Holes in 'pnadmin', 'dl-util', 'dl-search' and Other Scripts Let Remote Users Inject S
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](#) 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](#)