



CVE-2006-4202

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

Summary

CVE	CVE-2006-4202
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-17 21:04:00 UTC
Updated	2017-10-19 01:29:00 UTC
Description	SQL injection vulnerability in proje_goster.php in Spidey Blog Script 1.5 and earlier allows remote attackers to execute arbit

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spidey Blog	Spidey Blog Script	All	All	All	All

References

Reference	Source	Link
Spidey Blog Script <= 1.5 (tr) Remote SQL Injection Vulnerability	EXPLOIT-DB	www.exploit-db.com/exploits/1014
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/1014
Spidey Blog Script "pid" SQL Injection Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com/advisories/3714
Spidey Blog Script PID Parameter SQL Injection Vulnerability	BID	www.securityfocus.com/bid/1014
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve-2006-4202
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2006-4202

No vendor comments have been submitted for this CVE.

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

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