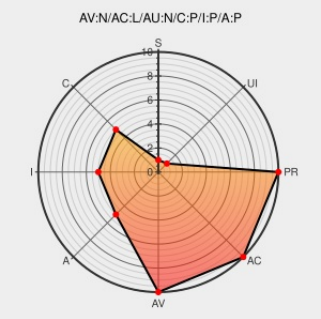
CVE-2005-2152

Published on: 07/06/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

CVE-2005-2152

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Geeklog from Geeklog contain the following vulnerability:

SQL injection vulnerability in Geeklog before 1.3.11 allows remote attackers to execute arbitrary SQL commands via user comments for an article.

CVE-2005-2152 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - Geeklog Unspecified SQL Injection Vulnerability	web.archive.org, text/html	SECUNIA 15914
Geeklog - Geeklog 1.3.11sr1 and 1.3.9sr4	Patch, Vendor Advisory, www.geeklog.net, text/html	CONFIRM www.geeklog.net/article.php/geeklog-1.3.11sr1
Hardened-PHP Project - PhP Security - Advisory 06/2005	Patch, Vendor Advisory, www.hardened-php.net, text/html	MISC www.hardened-php.net/advisory-062005.php
Geeklog Input Validation Hole When Retrieving Article Comments Permits SQL Injection Attacks - SecurityTracker	securitytracker.com, text/html	SECTRACK 1014381

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Geeklog	Geeklog	1.3.10	All	All	All
Application	Geeklog	Geeklog	1.3.6	All	All	All
Application	Geeklog	Geeklog	1.3.7	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr5	All	All	All
Application	Geeklog	Geeklog	1.3.8	All	All	All
Application	Geeklog	Geeklog	1.3.8_1	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr5	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr6	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.10	All	All	All
Application	Geeklog	Geeklog	1.3.6	All	All	All
Application	Geeklog	Geeklog	1.3.7	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.7_sr5	All	All	All
Application	Geeklog	Geeklog	1.3.8	All	All	All

Application	Geeklog	Geeklog	1.3.8_1	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr3	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr4	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr5	All	All	All
Application	Geeklog	Geeklog	1.3.8_1_sr6	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr1	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr2	All	All	All
Application	Geeklog	Geeklog	1.3.9_sr3	All	All	All

cpe:2.3:a:geeklog:geeklog:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7_sr1:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7_sr2:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7_sr3:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7_sr4:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.7_sr5:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr1:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr2:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr3:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr4:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr5:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr6:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.9_sr1:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.9_sr2:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.9_sr3:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:geeklog:geeklog:1.3.6:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7_sr1:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7_sr2:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7_sr3:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7_sr4:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.7_sr5:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr1:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr2:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr3:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr4:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr5:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.8_1_sr6:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.9_sr1:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.9_sr2:*:*:*:*:*:*:*

cpe:2.3:a:geeklog:geeklog:1.3.9_sr3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→