



CVE-2005-3022

Published on: 09/21/2005 12:00:00 AM UTC

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

CVE-2005-3022

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Vbulletin](#) from [Jelsoft](#) contain the following vulnerability:

Multiple SQL injection vulnerabilities in vBulletin 3.0.9 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) announcement parameter to announcement.php, (2) userid parameter to user.php, (3) calendar parameter to admincalendar.php, (4) cronid parameter to cronlog.php, (5) usergroupid parameter to email.php, (6) help parameter to help.php, (7) rvt parameter to language.php, (8) keep parameter to phrase.php, or (9) updateprofilepic parameter to usertools.php.

CVE-2005-3022 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[Exploit](#)
[Vendor Advisory](#)
[morph3us.org](#)
[text/plain](#)

[MISC morph3us.org/advisories/20050917-vbulletin-3.0.8.txt](#)

'[BuHa-Security] Multiple vulnerabilities in (admincp/modcp of)' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050918 \[BuHa-Security\] Multiple vulnerabilities in \(admincp/modcp of\) vBulletin 3.0.8/9](#)

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	Jelsoft	Vbulletin	1.0.1	All	lite	All
Application	Jelsoft	Vbulletin	2.0.3	All	All	All
Application	Jelsoft	Vbulletin	2.0_rc2	All	All	All
Application	Jelsoft	Vbulletin	2.0_rc3	All	All	All
Application	Jelsoft	Vbulletin	2.2.0	All	All	All
Application	Jelsoft	Vbulletin	2.2.1	All	All	All
Application	Jelsoft	Vbulletin	2.2.2	All	All	All
Application	Jelsoft	Vbulletin	2.2.3	All	All	All
Application	Jelsoft	Vbulletin	2.2.4	All	All	All
Application	Jelsoft	Vbulletin	2.2.5	All	All	All
Application	Jelsoft	Vbulletin	2.2.6	All	All	All
Application	Jelsoft	Vbulletin	2.2.7	All	All	All
Application	Jelsoft	Vbulletin	2.2.8	All	All	All
Application	Jelsoft	Vbulletin	2.2.9	All	All	All
Application	Jelsoft	Vbulletin	2.3.0	All	All	All
Application	Jelsoft	Vbulletin	2.3.2	All	All	All
Application	Jelsoft	Vbulletin	2.3.3	All	All	All
Application	Jelsoft	Vbulletin	2.3.4	All	All	All
Application	Jelsoft	Vbulletin	3.0	All	All	All
Application	Jelsoft	Vbulletin	3.0.1	All	All	All
Application	Jelsoft	Vbulletin	3.0.2	All	All	All
Application	Jelsoft	Vbulletin	3.0.3	All	All	All
Application	Jelsoft	Vbulletin	3.0.4	All	All	All
Application	Jelsoft	Vbulletin	3.0.5	All	All	All
Application	Jelsoft	Vbulletin	3.0.6	All	All	All
Application	Jelsoft	Vbulletin	3.0.7	All	All	All
Application	Jelsoft	Vbulletin	3.0.8	All	All	All
Application	Jelsoft	Vbulletin	3.0.9	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_2	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_3	All	All	All

Application	Jelsoft	Vbulletin	3.0_beta_4	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_5	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_6	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_7	All	All	All
Application	Jelsoft	Vbulletin	3.0_gamma	All	All	All
Application	Jelsoft	Vbulletin	1.0.1	All	lite	All
Application	Jelsoft	Vbulletin	2.0.3	All	All	All
Application	Jelsoft	Vbulletin	2.0_rc2	All	All	All
Application	Jelsoft	Vbulletin	2.0_rc3	All	All	All
Application	Jelsoft	Vbulletin	2.2.0	All	All	All
Application	Jelsoft	Vbulletin	2.2.1	All	All	All
Application	Jelsoft	Vbulletin	2.2.2	All	All	All
Application	Jelsoft	Vbulletin	2.2.3	All	All	All
Application	Jelsoft	Vbulletin	2.2.4	All	All	All
Application	Jelsoft	Vbulletin	2.2.5	All	All	All
Application	Jelsoft	Vbulletin	2.2.6	All	All	All
Application	Jelsoft	Vbulletin	2.2.7	All	All	All
Application	Jelsoft	Vbulletin	2.2.8	All	All	All
Application	Jelsoft	Vbulletin	2.2.9	All	All	All
Application	Jelsoft	Vbulletin	2.3.0	All	All	All
Application	Jelsoft	Vbulletin	2.3.2	All	All	All
Application	Jelsoft	Vbulletin	2.3.3	All	All	All
Application	Jelsoft	Vbulletin	2.3.4	All	All	All
Application	Jelsoft	Vbulletin	3.0	All	All	All
Application	Jelsoft	Vbulletin	3.0.1	All	All	All
Application	Jelsoft	Vbulletin	3.0.2	All	All	All
Application	Jelsoft	Vbulletin	3.0.3	All	All	All
Application	Jelsoft	Vbulletin	3.0.4	All	All	All
Application	Jelsoft	Vbulletin	3.0.5	All	All	All
Application	Jelsoft	Vbulletin	3.0.6	All	All	All
Application	Jelsoft	Vbulletin	3.0.7	All	All	All
Application	Jelsoft	Vbulletin	3.0.8	All	All	All
Application	Jelsoft	Vbulletin	3.0.9	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_2	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_3	All	All	All

Application	Jelsoft	Vbulletin	3.0_beta_4	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_5	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_6	All	All	All
Application	Jelsoft	Vbulletin	3.0_beta_7	All	All	All
Application	Jelsoft	Vbulletin	3.0_gamma	All	All	All
cpe:2.3:a:jelsoft:vbulletin:1.0.1:*:lite:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.0.3:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.0_rc2:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.0_rc3:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.0:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.1:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.2:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.3:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.4:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.5:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.6:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.7:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.8:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.2.9:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.3.0:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.3.2:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.3.3:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:2.3.4:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.1:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.2:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.3:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.4:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.5:*:*:*:*:*:*						
cpe:2.3:a:jelsoft:vbulletin:3.0.6:*:*:*:*:*:*						

cpe:2.3:a:jelsoft:bulletin:3.0.7:*****:
cpe:2.3:a:jelsoft:bulletin:3.0.8:*****:
cpe:2.3:a:jelsoft:bulletin:3.0.9:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_2:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_3:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_4:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_5:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_6:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_beta_7:*****:
cpe:2.3:a:jelsoft:bulletin:3.0_gamma:*****:
cpe:2.3:a:jelsoft:bulletin:1.0.1:lite:*****:
cpe:2.3:a:jelsoft:bulletin:2.0.3:*****:
cpe:2.3:a:jelsoft:bulletin:2.0_rc2:*****:
cpe:2.3:a:jelsoft:bulletin:2.0_rc3:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.0:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.1:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.2:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.3:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.4:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.5:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.6:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.7:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.8:*****:
cpe:2.3:a:jelsoft:bulletin:2.2.9:*****:
cpe:2.3:a:jelsoft:bulletin:2.3.0:*****:
cpe:2.3:a:jelsoft:bulletin:2.3.2:*****:
cpe:2.3:a:jelsoft:bulletin:2.3.3:*****:
cpe:2.3:a:jelsoft:bulletin:2.3.4:*****:

cpe:2.3:a:jelsoft:vbulletin:3.0:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.1:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.2:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.3:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.4:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.5:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.6:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.7:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.8:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0.9:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_2:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_3:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_4:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_5:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_6:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_beta_7:*****:
cpe:2.3:a:jelsoft:vbulletin:3.0_gamma:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)