



CVE-2006-1094

Published on: 03/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1094

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

Certain versions of [Datenbank Module](#) from [Datenbank Module](#) contain the following vulnerability:

SQL injection vulnerability in Datenbank MOD 2.7 and earlier for Woltlab Burning Board allows remote attackers to execute arbitrary SQL commands via the fileid parameter to (1) info_db.php or (2) database.php.

CVE-2006-1094 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

SecurityFocus

[Exploit](#)
[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20060301 Woltlab Burning Board 2.x \(Datenbank MOD fileid\) Multiple Vulnerabilities](#)

Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers

[www.nukedx.com](#)
[text/xml](#)

[MISC www.nukedx.com/?viewdoc=17](#)

Woltlab Burning Board Multiple SQL Injection Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[BID 16914](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 23810](#)

[Inactive Link](#) [Not Archived](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 23808](#)

[Inactive Link](#) [Not Archived](#)

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	Datenbank Module	Datenbank Module	All	All	All	All
Application	Woltilab	Burning Board	1.1.1	All	All	All
Application	Woltilab	Burning Board	2.0_beta_3	All	All	All
Application	Woltilab	Burning Board	2.0_beta_4	All	All	All
Application	Woltilab	Burning Board	2.0_beta_5	All	All	All
Application	Woltilab	Burning Board	2.0_rc1	All	All	All
Application	Woltilab	Burning Board	2.0_rc2	All	All	All
Application	Woltilab	Burning Board	2.2.2	All	All	All
Application	Woltilab	Burning Board	2.3.1	All	All	All
Application	Woltilab	Burning Board	2.3.3	All	All	All
Application	Woltilab	Burning Board	2.4	All	All	All
Application	Woltilab	Burning Board	2.5	All	All	All
Application	Woltilab	Burning Board	2.6	All	All	All
Application	Woltilab	Burning Board	2.7	All	All	All
Application	Woltilab	Burning Board	1.1.1	All	All	All
Application	Woltilab	Burning Board	2.0_beta_3	All	All	All
Application	Woltilab	Burning Board	2.0_beta_4	All	All	All
Application	Woltilab	Burning Board	2.0_beta_5	All	All	All
Application	Woltilab	Burning Board	2.0_rc1	All	All	All
Application	Woltilab	Burning Board	2.0_rc2	All	All	All
Application	Woltilab	Burning Board	2.2.2	All	All	All
Application	Woltilab	Burning Board	2.3.1	All	All	All
Application	Woltilab	Burning Board	2.3.3	All	All	All
Application	Woltilab	Burning Board	2.4	All	All	All
Application	Woltilab	Burning Board	2.5	All	All	All
Application	Woltilab	Burning Board	2.6	All	All	All
Application	Woltilab	Burning Board	2.7	All	All	All

cpe:2.3:a:datenbank_module:datenbank_module:*****:
cpe:2.3:a:woltlab:burning_board:1.1.1:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_3:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_4:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_5:*****:
cpe:2.3:a:woltlab:burning_board:2.0_rc1:*****:
cpe:2.3:a:woltlab:burning_board:2.0_rc2:*****:
cpe:2.3:a:woltlab:burning_board:2.2.2:*****:
cpe:2.3:a:woltlab:burning_board:2.3.1:*****:
cpe:2.3:a:woltlab:burning_board:2.3.3:*****:
cpe:2.3:a:woltlab:burning_board:2.4:*****:
cpe:2.3:a:woltlab:burning_board:2.5:*****:
cpe:2.3:a:woltlab:burning_board:2.6:*****:
cpe:2.3:a:woltlab:burning_board:2.7:*****:
cpe:2.3:a:woltlab:burning_board:1.1.1:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_3:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_4:*****:
cpe:2.3:a:woltlab:burning_board:2.0_beta_5:*****:
cpe:2.3:a:woltlab:burning_board:2.0_rc1:*****:
cpe:2.3:a:woltlab:burning_board:2.0_rc2:*****:
cpe:2.3:a:woltlab:burning_board:2.2.2:*****:
cpe:2.3:a:woltlab:burning_board:2.3.1:*****:
cpe:2.3:a:woltlab:burning_board:2.3.3:*****:
cpe:2.3:a:woltlab:burning_board:2.4:*****:
cpe:2.3:a:woltlab:burning_board:2.5:*****:
cpe:2.3:a:woltlab:burning_board:2.6:*****:
cpe:2.3:a:woltlab:burning_board:2.7:*****:

© [CVE.report](#) 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)