



CVE-2005-3518

Published on: 11/06/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-3518

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

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

SQL injection vulnerability in search.php in PunBB 1.2.7 and 1.2.8 allows remote attackers to execute arbitrary SQL commands via the old_searches parameter.

CVE-2005-3518 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

KAPDA :: Punbb search.php SQL_Injection

[Exploit](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#) [www.kapda.ir/advisory-91.html](#)

[No Description Provided](#)

[www.osvdb.org](#)
[Inactive Link](#) [Not Archived](#)

[OSVDB](#) 20018

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF](#) [punbb-oldsearches-sql-injection\(22760\)](#)

Punbb SQL Injection Vulnerability - SecurityReason.com

[securityreason.com](#)
[text/html](#)

[SREASON](#) 87

[www.punbb.org](#)

[CONFIRM](#)

[text/plain](#)[Inactive Link](#) [Not Archived](#)www.punbb.org/changelogs/1.2.8_to_1.2.9.txt

'[KAPDA::#6] Punbb SQL Injection Vulnerability' - MARC

[marc.info](#)[text/html](#)[BUGTRAQ 20051014 \[KAPDA::#6\] Punbb SQL Injection Vulnerability](#)

PunBB Search.PHP SQL Injection Vulnerability

[Exploit](#)[Patch](#)[web.archive.org](#)[text/html](#)[Inactive Link](#) [Not Archived](#)[BID 15114](#)

Secunia - Advisories - PunBB "old_searches" SQL Injection Vulnerability

[Patch](#)[Vendor Advisory](#)[web.archive.org](#)[text/html](#)[SECUNIA 17227](#)

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	Punbb	Punbb	1.2.7	All	All	All
Application	Punbb	Punbb	1.2.8	All	All	All
Application	Punbb	Punbb	1.2.7	All	All	All
Application	Punbb	Punbb	1.2.8	All	All	All

cpe:2.3:a:punbb:punbb:1.2.7:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.8:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.7:*:*:*:*:*:

cpe:2.3:a:punbb:punbb:1.2.8:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)© 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](#).

