



CVE-2005-3259

Published on: 10/20/2005 12:00:00 AM UTC

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

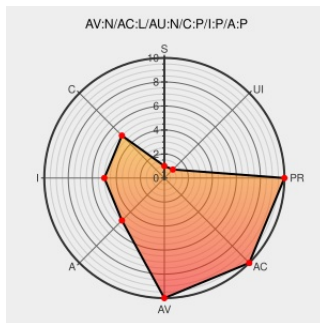
CVE-2005-3259

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Multiple SQL injection vulnerabilities in versatileBulletinBoard (vBB) 1.0.0 RC2 allow remote attackers to execute arbitrary SQL commands and bypass authentication via the (1) login field, (2) "search this thread" feature, (3) "search for posts" feature, (4) "forgot password" feature, (5) list parameter in userlistpre.php, and the (6) select, (7) categ, and (8) to parameters in index.php.

CVE-2005-3259 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

No Description Provided

[www.osvdb.org](#)

[OSVDB 19968](#)

Inactive Link Not Archived

VersatileBulletinBoard Multiple SQL Injection Vulnerabilities

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

[BID 15068](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 19966](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 19963](#)

	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 19964
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 19967
	Inactive Link Not Archived	
No Description Provided	Exploit Vendor Advisory rgod.altervista.org	MISC rgod.altervista.org/versatile100RC2.html
	Inactive Link Not Archived	
Secunia - Advisories - versatileBulletinBoard Cross-Site Scripting and SQL Injection	Vendor Advisory web.archive.org text/html	SECUNIA 17174
No Description Provided	www.osvdb.org	OSVDB 19965
	Inactive Link Not Archived	
No Description Provided	www.osvdb.org	OSVDB 19962
	Inactive Link Not Archived	
'versatileBulletinBoard V1.0.0 RC2 (possibly prior versions)' - MARC	marc.info text/html	BUGTRAQ 20051010 versatileBulletinBoard V1.0.0 RC2 (possibly prior versions)

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	Versatilebulletinboard	Versatilebulletinboard	1.0.0.rc2	All	All	All
Application	Versatilebulletinboard	Versatilebulletinboard	1.0.0.rc2	All	All	All
cpe:2.3:a:versatilebulletinboard:versatilebulletinboard:1.0.0.rc2:*****:						
cpe:2.3:a:versatilebulletinboard:versatilebulletinboard:1.0.0.rc2:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)