



CVE-2013-3563

Published on: 07/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-3563

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

Certain versions of [Lianja Sql Server](#) from [Lianja](#) contain the following vulnerability:

Stack-based buffer overflow in db_netserver in Lianja SQL Server before 1.0.0RC5.2 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted string to TCP port 8001.

CVE-2013-3563 has been assigned by [M](#) 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

Lianja SQL 1.0.0RC5.1 - db_netserver Stack Buffer Overflow (Metasploit) - Windows remote Exploit

[Exploit](#)

[www.exploit-db.com](#)

[Proof of Concept](#)

[text/html](#)

[EXPLOIT-DB](#)
25851

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)

Known/Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lianja	Lianja Sql Server	All	rc5.1	All	All
cpe:2.3:a:lianja:lianja_sql_server:*:rc5.1:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)