

[NEWS] SQL Injection in package MDSYS.SDO_LRS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00089.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 24 Oct 2006 12:12:12 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

SQL Injection in package MDSYS.SDO_LRS

SUMMARY

The package MDSYS.SDO_LRS contains a SQL injection vulnerability in the first parameter of convert_to_lrs_layer. Oracle forgot to fix this problem with the April CPU. Oracle fixed these vulnerabilities with the package DBMS_ASSERT. To exploit this vulnerability it is necessary to have the privilege to create a PL/SQL-function.

DETAILS

Vulnerable Systems:
* Oracle 9i Rel. 2

Sample:

After running the following SQL statement
select sdo_lrs.convert_to_lrs_layer('"' or
5=5--"'', 'RDS', 'A', 1, 1, 1, 1) from dual;

The following SQL statement will be executed by Oracle:
SELECT COUNT(*) FROM USER_SDO_INDEX_INFO WHERE TABLE_NAME = '"' OR
5=5--"' AND COLUMN_NAME = 'RDS'

[NEWS] SQL Injection in package MDSYS.SDO_LRS

Patch Information:

Apply the patches for Oracle CPU October 2006.

History

- 19-apr-2006 Oracle secalert was informed
- 18-oct-2006 Oracle published CPU October 2006 [DB13]
- 18-oct-2006 Advisory published

ADDITIONAL INFORMATION

The information has been provided by <<mailto:k@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>>
Alexander Kornbrust.

The original article can be found at:

<http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_lrs.html>
http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_lrs.html

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.