

[NEWS] Oracle Reports Lexical References SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0068.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/19/05

To: list@securiteam.com

Date: 19 Sep 2005 10:22:13 +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>

Oracle Reports Lexical References SQL Injection

SUMMARY

<<http://www.oracle.com/technology/products/reports/>> Oracle Reports is "Oracle's award-winning, high-fidelity enterprise reporting tool. It enables businesses to give immediate access to information to all levels within and outside of the organization in an unrivaled scalable and secure environment".

Self developed Oracle Reports are vulnerable against SQL Injection if these reports are using lexical references without input validation. Most Oracle reports developers are not aware of this problem and are not validating the input (e.g. from parameters) in Oracle Reports. As every input validation bug it is not a problem of the development tool itself (in this case Oracle Reports Developer) it is a problem of the developers using Oracle Reports developer. The Oracle documentation holds back information about this potential problem.

DETAILS

Vulnerable Systems:

- * All generated Oracle reports using lexical reference since Oracle

Securiteam: [NEWS] Oracle Reports Lexical References SQL Injection

Reports version 2.0

Oracle Reports are created with the Oracle Reports developer and are quite common in the enterprise environment. Oracle itself is using Oracle Reports e.g. in their E-Business-Suite. Oracle Reports provides a feature called lexical references. A lexical reference is a placeholder for text that you embed in a SELECT statement. It is possible to replace the clauses appearing after SELECT, FROM, WHERE, GROUP BY, ORDER BY, HAVING, CONNECT BY and START WITH.

Short demonstration of SQL Injection in Oracle Reports:

The following vulnerable sample report for the demo user scott/tiger can be downloaded from :

<http://www.red-database-security.com/wp/demo_sql_injection_reports.zip>
http://www.red-database-security.com/wp/demo_sql_injection_reports.zip

To run this report an Oracle Reportsserver is required.

1. Run an Oracle Reports via a web browser

<http://myserver:8889/reports/rwservlet?report=sqlinject3.rdf+userid=scott/tiger@ora9206+destype=CACHE+desformat=HTML>

2. Add the parameter paramform=yes to the URL and resubmit the URL again.

A HTML window appears which allows a user to modify parameter values from a web page, e.g. change the sort sequence (e.g. ORDER BY ENAME)

3. Replace the default value ORDER BY 1 of the parameter P_WHERE with the string UNION select NULL,USERNAME, NULL,NULL,NULL,NULL,NULL,NULL from all_users.

If the resulting SQL statement is not correct Oracle reports returns the appropriate error message (e.g. REP-300)

4. Submit the modified query. Oracle Reports server replaces the parameter P_WHERE with the value submitted by the URL and executes the statement.

Fix:

It is not possible to disable the lexical references functionality by setting a special environment variable. It is necessary to fix this problem in every report by validating every parameter in an After-Parameter-Form-Trigger.

This can be time consuming task if you check several hundreds of reports.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:ak@red-database-security.com>> Kornbrust, Alexander.

The original article can be found at:

<http://www.red-database-security.com/wp/sql_injection_reports_us.pdf>
http://www.red-database-security.com/wp/sql_injection_reports_us.pdf

=====

Securiteam: [NEWS] Oracle Reports Lexical References SQL Injection

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.