

# [NEWS] Oracle SQL Injection Possible Via CTXSYS.DRILOAD

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0022.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/12/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 12 Sep 2004 10:46:03 +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 SQL Injection Possible Via CTXSYS.DRILOAD

---

## SUMMARY

An SQL injection vulnerability was found in the <<http://www.oracle.com>> Oracle Database Server through the abuse of parameters in the DRILOAD package.

## DETAILS

### Vulnerable Systems:

- \* Oracle Database Server 8i (All platforms)
- \* Oracle Database Server 9i (All platforms)

### Immune Systems:

- \* Oracle Database Server 10g

The vulnerability allows any valid database user to gain DBA rights over the database if CTXSYS is installed, by executing the DRILOAD package using a specially crafted parameter passed to it.

### Workaround

The following workarounds are possible for vulnerable versions of Oracle:

Securiteam: [NEWS] Oracle SQL Injection Possible Via CTXSYS.DRILOAD

- \* Drop the CTXSYS user if it's not needed.
- \* Revoke public grant from CTXSYS.DRILOAD and limit access to it by allowing trusted users only.

Patch Availability:

Please see MetaLink Document ID 281189.1 for the patch download procedures and for the Patch Availability Matrix for this Oracle Security Alert which can be found at:

<[http://metalink.oracle.com/metalink/plsql/ml2\\_documents.showDocument?p\\_database\\_id=NOT&p\\_id=281189.1](http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1)>  
[http://metalink.oracle.com/metalink/plsql/ml2\\_documents.showDocument?p\\_database\\_id=NOT&p\\_id=281189.1](http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1)

Disclosure Timeline

- 5 Januar 2004 Oracle was informed
- 6 Januar 2004 Bug confirmed
- 31 August 2004 Oracle published alert 68

ADDITIONAL INFORMATION

The information has been provided by <mailto:ak@red-database-security.com> Kornbrust, Alexander – Red Database Security.

The original article can be found at:

<[http://www.red-database-security.com/advisory/advisory\\_20040903\\_1.htm](http://www.red-database-security.com/advisory/advisory_20040903_1.htm)>  
[http://www.red-database-security.com/advisory/advisory\\_20040903\\_1.htm](http://www.red-database-security.com/advisory/advisory_20040903_1.htm)

=====

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.