

[UNIX] Oracle Database Buffer Overflow Vulnerabilities in Procedure DBMS_DRS.GET_PROPERTY (DB03)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-07/msg00054.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jul 2007 15:14:32 +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 Database Buffer Overflow Vulnerabilities in Procedure
DBMS_DRS.GET_PROPERTY (DB03)

SUMMARY

Oracle Database Server provides the DBMS_DRS package that includes procedures used in Oracle Data Guard. This package contains the function GET_PROPERTY which is vulnerable to buffer overflow attacks.

DETAILS

Vulnerable Systems:

* Oracle Database Server versions 9i, 9iR2, 10gR1 and 10gR2

Impact:

Any Oracle database user with EXECUTE privilege on the package SYS.DBMS_DRS can exploit this vulnerability. Exploitation of this vulnerability allows an attacker to execute arbitrary code. It can also be exploited to cause DOS (Denial of service) killing Oracle server process.

Vendor Status:

[UNIX] Oracle Database Buffer Overflow Vulnerabilities in Procedure DBMS_DRS.GET_PROPERTY (DB03)

Vendor was contacted and a patch was released.

Workaround:

Restrict access to the SYS.DBMS_DRS package.

Fix:

Apply Oracle Critical Patch Update July 2007 available at Oracle Metalink:

<http://www.oracle.com/technology/deplo/security/critical-patch-updates/cpujul2007.html>
<http://www.oracle.com/technology/deplo/security/critical-patch-updates/cpujul2007.html>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0270>
CVE-2007-0270

ADDITIONAL INFORMATION

The information has been provided by <mailto:shatter@xxxxxxxxxxxxxx> Team SHATTER.

The original article can be found at:

<http://www.appsecinc.com/resources/alerts/oracle/2007-04.shtml>
<http://www.appsecinc.com/resources/alerts/oracle/2007-04.shtml>

=====

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.