

# [VulnWatch] Oracle Database Buffer overflow vulnerabilities in procedure DBMS\_DRS.GET\_PROPERTY (DB03)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-07/msg00026.html>

---

- *From:* Team SHATTER <[shatter@xxxxxxxxxxxxx](mailto:shatter@xxxxxxxxxxxxx)>
  - *Date:* Wed, 18 Jul 2007 17:52:12 -0400
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Team SHATTER Security Alert (Update)

Oracle Database Buffer overflow vulnerabilities in procedure  
DBMS\_DRS.GET\_PROPERTY (DB03)

Jan 18, 2007 (Updated July 18th, 2007)

Risk Level: Medium

Affected versions:

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

Remote exploitable: Yes (Authentication to Database Server is needed)

Credits:

This vulnerability was discovered and researched by Esteban Martínez  
Fayó of Application Security Inc.

CVE:

CVE-2007-0270

Details:

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.

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:

[VulnWatch] 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.

Links:

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

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

-- --

---

Application Security, Inc.

[www.appsecinc.com](http://www.appsecinc.com)

AppSecInc is the leading provider of database security solutions for the enterprise. AppSecInc products proactively secure enterprise applications at more than 300 organizations around the world by discovering, assessing, and protecting the database against rapidly changing security threats. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.7 (MingW32)

iD8DBQFGnouL9EOAcmTuFN0RAve6AJ9czDnP5Pi+1udZOwhhgIZgxWASMACg1t2u  
XMXFWDANEjUSXMvrEmPgk+I=  
=Fkhp

-----END PGP SIGNATURE-----

**Attachment:** [0x64EE14DD.asc](#)

*Description:* application/pgp-keys

[VulnWatch] Oracle Database Buffer overflow vulnerabilities in procedure DBMS\_DRS.GET\_PROPERTY (DB03)