

# [VulnWatch] Oracle Database Buffer overflow vulnerabilities in package DBMS\_SNAP\_INTERNAL

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-04/msg00023.html>

---

- *From:* Team SHATTER <[shatter@xxxxxxxxxxxxxx](mailto:shatter@xxxxxxxxxxxxxx)>
  - *Date:* Wed, 18 Apr 2007 14:20:58 -0400
- 

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

Hash: SHA1

Title: Oracle Database Buffer overflow vulnerabilities in package DBMS\_SNAP\_INTERNAL

Risk Level: Medium

Affected versions:

Oracle Database Server versions 8i, 9i and 10gR1

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

Credits:

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

Details:

Oracle Database Server provides the DBMS\_SNAP\_INTERNAL package that contains procedures used internally by Oracle. Some procedures of this package have the parameters SNAP\_OWNER and SNAP\_NAME. These parameters are vulnerable to buffer overflow attacks.

Impact:

Any Oracle database user with EXECUTE privilege on the package SYS.DBMS\_SNAP\_INTERNAL 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 the Oracle server process.

Vendor Status:

Vendor was contacted and a patch was released.

Workaround:

Restrict access to the SYS.DBMS\_SNAP\_INTERNAL package.

Fix:

Apply Oracle Critical Patch Update April 2007 available at Oracle Metalink.

[VulnWatch] Oracle Database Buffer overflow vulnerabilities in package DBMS\_SNAP\_INTERNAL

Links:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html>

<http://www.appsecinc.com/resources/alerts/oracle/2007-07.shtml>

---

Application Security, Inc.

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)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iD8DBQFGJmGK9EOAcmTuFN0RAm4qAJwMWIuqw1wETWxS7nSFrOyPx/WJWgCgoRQz  
q8l1BKUahqqkGZvHT6x3CEQ=  
=RbmR

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

**Attachment: 0x64EE14DD.asc**

*Description:* application/pgp-keys

[VulnWatch] Oracle Database Buffer overflow vulnerabilities in package DBMS\_SNAP\_INTERNAL 2