

# US-CERT Technical Cyber Security Alert TA06-018A -- Oracle Products Contain Multiple Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Cert/2006-01/msg00003.html>

---

- *From:* CERT Advisory <[cert-advisory@xxxxxxxx](mailto:cert-advisory@xxxxxxxx)>
  - *Date:* Wed, 18 Jan 2006 17:11:24 -0500
- 

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

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA06-018A

Oracle Products Contain Multiple Vulnerabilities

Original release date: January 18, 2006

Last revised: --

Source: US-CERT

Systems Affected

- \* Oracle Database 10g
- \* Oracle9i Database
- \* Oracle8i Database
- \* Oracle Enterprise Manager 10g Grid Control
- \* Oracle Application Server 10g
- \* Oracle9i Application Server
- \* Oracle Collaboration Suite 10g
- \* Oracle9i Collaboration Suite
- \* Oracle E-Business Suite Release 11i
- \* Oracle E-Business Suite Release 11.0
- \* JD Edwards EnterpriseOne, OneWorld Tools
- \* PeopleSoft Enterprise Portal
- \* Oracle Workflow

For more information regarding affected product versions, please see the Oracle Critical Patch Update - January 2006.

## Overview

Various Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial of service.

## I. Description

Oracle has released Critical Patch Update – January 2006. This update addresses more than eighty vulnerabilities in different Oracle products and components.

The Critical Patch Update provides information about affected components, access and authorization required, and the impact of the vulnerabilities on data confidentiality, integrity, and availability. For more information on terms used in the Critical Patch Update, Metalink customers should refer to MetaLink Note 293956.1.

According to Oracle, three of the vulnerabilities corrected in the Oracle Critical Patch Update for January 2006 affect Oracle Database Client–only installations.

US–CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. US–CERT is tracking all of these issues under VU#545804. As further information becomes available, we will publish individual Vulnerability Notes.

## II. Impact

The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include the execution of arbitrary code or commands, information disclosure, and denial of service. Vulnerable components are likely to be available to attackers via remote networks and with limited or no prior authorization. An attacker who compromises an Oracle database may be able to gain access to sensitive information.

## III. Solution

### Apply a patch

Apply the appropriate patches or upgrade as specified in the Oracle Critical Patch Update – January 2006. Note that this Critical Patch Update only lists newly corrected issues. Updates to patches for previously known issues are not listed.

## US-CERT Technical Cyber Security Alert TA06-018A -- Oracle Products Contain Multiple Vulnerabilities

As noted in the update, some patches are cumulative, others are not:

The Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne and OneWorld Tools, and PeopleSoft Enterprise Portal Applications patches in the Updates are cumulative; each successive Critical Patch Update contains the fixes from the previous Critical Patch Updates.

Oracle E-Business Suite and Applications patches are not cumulative, so E-Business Suite and Applications customers should refer to previous Critical Patch Updates to identify previous fixes they wish to apply.

### Appendix A. Vendor Information

#### Oracle

Please see Oracle Critical Patch Update – January 2006 and Critical Patch Updates and Security Alerts.

### Appendix B. References

\* Critical Patch Update – January 2006 –

<<http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>>

\* Critical Patch Updates and Security Alerts –

<<http://www.oracle.com/technology/deploy/security/alerts.htm>>

\* MetaLink Note 293956.1 –

<<http://metalink.oracle.com/metalink/plsql/showdoc?db=Not&id=293956.1>>

\* US-CERT Vulnerability Note VU#545804 –

<<http://www.kb.cert.org/vuls/id/545804>>

\* US-CERT Vulnerability Notes Related to Critical Patch Update – January 2006 –

<[http://www.kb.cert.org/vuls/byid?searchview&query=oracle\\_cpu\\_january\\_2006](http://www.kb.cert.org/vuls/byid?searchview&query=oracle_cpu_january_2006)>

\* Map of Public Vulnerability to Advisory/Alert –

<[http://www.oracle.com/technology/deploy/security/pdf/public\\_vuln\\_to\\_advisory\\_mapping.html](http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html)>

\* Oracle Database Security Checklist (PDF) –

<[http://www.oracle.com/technology/deploy/security/pdf/twp\\_security\\_checklist\\_db\\_database.pdf](http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf)>

Information used in this document came from Oracle.

Oracle credits the following individuals for providing information regarding vulnerabilities addressed in the Critical Patch Update – January 2006: Raffaele Amendola; Cesar Cerrudo and Esteban Martinez Fayo of Application Security, Inc.; Joxean Koret; Alexander Kornbrust of Red Database Security GmbH; David Litchfield of Next Generation Security Software Ltd.; Srinivas Nookala of Cenxic, Inc.; Steve Orrin formally of Watchfire, Inc.; Amichai Shulman of Imperva, Inc. Feedback can be directed to US-CERT Technical Staff.

---

The most recent version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA06-018A.html>>

---

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@xxxxxxxx> with "TA06-018A Feedback VU#545804" in the subject.

---

For instructions on subscribing to or unsubscribing from this mailing list, visit <<http://www.us-cert.gov/cas/signup.html>>.

---

Produced 2006 by US-CERT, a government organization.

Terms of use:

<<http://www.us-cert.gov/legal.html>>

---

#### Revision History

January 18, 2006: Initial release

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

Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBQ866SH0pj593lg50AQJQtwgAzAwHvbTaulcH4R76IfBf2K/QLMma7b9B  
omvFWMOnCICUDvkLvW2dGBOPJZjmluQz6154w2OfsiHhpHzjlmEjbJKQ1kVWjKI  
o+k3GcCZiZByEORtcKDpIjZ6U4c4+ZOdy7B/kEdEMOR1kPr2WLF9uZCkKsqxnd  
Nm//1GkNC77+NGdhqhdIqcFyL7X1ZmHDNwAbZ9EmMO2Pc5a5ManLgW7LBnuxVzCv  
cj9dRYZvbatrr9P2sxaj7xBZgYoDwQW+s+oy/N77mva5K/IVLE67UIIm0Bj7h9gFiX  
dmF/bVU1wocLEHSPY0MqUySI99eJnZv4/IIM61/Moxb/TQ4xoiPsjA==  
=D3pG

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

---

- Prev by Date: [\*US-CERT Technical Cyber Security Alert TA06-011A -- Apple QuickTime Vulnerabilities\*](#)
- Previous by thread: [\*US-CERT Technical Cyber Security Alert TA06-011A -- Apple QuickTime Vulnerabilities\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)