UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−015

Múltiples vulnerabilidades en productos Oracle

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo informa que los productos Oracle y sus componentes son afectados por múltiples vulnerabilidades. El impacto de estas vulnerabilidades incluye la ejecución remota de código arbitrario, publicación de información y negación de servicio.

Fecha de Liberación: 19 de Abril de 2006

Ultima Revisión: 20 de Abril de 2006

Fuente: US−CERT

Sistemas Afectados

JD Edwards EnterpriseOne, OneWorld Tools	==8.95 − 8.95.J1
Oracle Application Server 10g	==10.1.2.0.0 − 10.1.2.0.2, 10.1.2.1.0, 10.1.3.0.0, 9.0.4.1, 9.0.4.2
Oracle Collaboration Suite 10g	==10.1.1, 10.1.2.0, 10.1.2.1
Oracle Database 10g	==10.2.0.1, 10.2.0.2, 10.1.0.4, 10.1.0.5
Oracle Developer Suite 6i	==9.0.4.2
Oracle E−Business Suite Release 11.0	==11.0
Oracle E−Business Suite Release 11i	==11.5.1 − 11.5.10 CU2
Oracle Enterprise Manager 10g Grid Control	==10.1.0.3, 10.1.0.4, 10.2.0.1, ==

Oracle PeopleSoft Enterprise Tools	8.47GA − 8.47.04, 8.46GA − 8.46.12
Oracle Pharmaceutical Applications	==4.5.0 − 4.5.2
Oracle Workflow	==11.5.1−11.5.9.5
Oracle8i Database	==8.1.7.4
Oracle9i Collaboration Suite	==9.0.4.2
Oracle9i Database	==9.2.0.6, 9.2.0.7

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución remota de código y negación de servicio

I. **Descripción**

Oracle ha publicado una actualización crítica − Abril de 2006. Esta actualización trata más de treinta vulnerabilidades en diferentes productos y componentes de Oracle.

La actualización crítica proporciona información acerca de componentes afectados, acceso y autorización requerida, además del impacto de las vulnerabilidades sobre la confidencialidad, disponibilidad e integridad de la información. Los clientes de MetaLink deben revisar la Nota MetalinK 293956.1 (login requerido) para obtener mayor información sobre los términos utilizados en las actualizaciones críticas.

De acuerdo con Oracle, ningúna de las vulnerabilidades corregidas en este paquete de actualizaciones afecta a la instalación de clientes de su base de datos.

La vulnerabilidad sobre PL/SQL identificada como PLSQL01 en el paquete de actualizaciones corresponde a la nota de vulnerabilidad US−CERT VU#169164, en la cual se incluyen detalles.

En la mayoría de los casos, Oracle no asocia los identificadores de la vulnerabilidad del tipo Vuln# (p.e.,DB01) con otra información disponible. Si surgen mayores detalles acerca de las vulnerabilidades y su estrategia de solución, se actulizará la información de este boletin.

II. **Impacto**

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y la configuración del sistema. Los riesgos potenciales incluye la ejecución remota de código arbitrario y de comandos, publicación de información y negación de servicio. Los componentes vulnerables podrían estar a disposición de los atacantes remotos. Un atacante que compromenta la base de datos Oracle podría tener acceso a información sensible.

III. Solución

Aplicar las actualizaciones.

Aplicar los parches o actualizaciones apropiadas como se especifica en Actualizaciones Críticas de Oracle − Abril de 2006. Se debe notar que estas actualizaciones criticas sólo listan las nuevas correcciones. La actualización de los parches para las ya conocidas no son listadas.

Es importante mencionar que algunas actualizaciones son acumulativas y otras no:

Las correcciones acumulativas son Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne and OneWorld Tools y PeopleSoft Enterprise Portal Applications; cada actualización crítica corrige la actualización crítica previa.

Oracle E−Business Suite y Applications no son correcciones acumulativas, por lo que es importante referirse a las actualizaciones críticas previas para identificar correcciones anteriores que deseen aplicar.

La actualizaciones para algunas plataformas y componentes no estaban disponibles cuando la actualización crítica fue publicada el 18 de abril de 2006. Favor ver la Nota MetaLink 360465.1 (login requerido) para más información.

Información adicional de las correcciones de Oracle son documentadas en las notas de pre−instalación y archivos "readme" de la actualización. Favor de consultar los documentos específicos de cada uno de los sistemas antes de aplicar las actualizaciones.

IV. Apéndice A. Información

Oracle

Favor de ver las Actualizaciones Críticas de Oracle de Abril de 2006, actualización de parches críticos y alertas de seguridad.

V. Apéndice B. Referencias

- Nota de vulnerabilidad US−CERT VU#169164 − http://www.kb.cert.org/vuls/id/169164
- Nota de vulnerabilidad US−CERT relacionada a las Actualizaciones Críticas de Abril de 2006 − http://www.kb.cert.org/vuls/byid?searchview_april_2006
- Actualizaciones Críticas de Abril de 2006 − http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html
- Actualización de parches críticos y Alertas de Seguridad − http://www.oracle.com/technology/deploy/security/alerts.htm
- Esquema de vulnerabilidades de avisos o alertas − http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html
- Checklist de seguridad para la base de datos Oracle (PDF) − http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- Nota MetaLink 293956.1 (login requerido) − http://metalink.oracle.com/metalink/plsql/showdoc?db=Not
- Nota MetaLink 360465.1 (login requerido) − http://metalink.oracle.com/metalink/plsql/showdoc?db=Not

- Detalles de la actualización crítica de Oracle de Abril de 2006 − http://www.red−database−security.com/advisory/oracle_cpu_apr_2006.html

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Sergio Alavez Miguel (salavez at seguridad dot unam dot mx)
- Ricardo Carrillo Sanchez (rcarrillo at correo dot seguridad dot unam dot mx)
- Juan Lopez Morales (jlopez at correo dot seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 43