UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−024

Productos Oracle contienen múltiples vulnerabilidades

Los productos y componentes Oracle son afectados por múltiples vulnerabilidades. Los impactos de éstas vulnerabilidades incluyen la ejecución remota de código arbitrario, revelación de información y negación de servicio.

Fecha de Liberación:	19 de Julio de 2006
Ultima Revisión:	20 de Julio de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Sistemas afectados**

- Oracle10*g* Database
- Oracle9*i* Database
- Oracle8*i* Database
- Oracle Enterprise Manager 10*g* Grid Control
- Oracle Application Server 10*g*
- Oracle Collaboration Suite 10*g*
- Oracle9*i* Collaboration Suite
- Oracle E−Business Suite Release 11*i*
- Oracle E−Business Suite Release 11.0
- Oracle Pharmaceutical Applications
- JD Edwards EnterpriseOne, OneWorld Tools
- Oracle PeopleSoft Enterprise Portal Solutions

Para mayor información sobre las versiones de los productos afectados, consulte la Actualización Crítica de Oracle − Julio de 2006.

II. Descripción

Oracle ha liberado la Actualización Crítica de Oracle − Julio de 2006. Esta actualización soluciona numerosas vulnerabilidades en diferentes productos y componentes de Oracle.

La Actualización Crítica proporciona información sobre componentes afectados, accesos y autorización requerida, y el impacto de vulnerabilidades en confidencialidad de datos, integridad y disponibilidad. Los usuarios de MetaLink deberían referirse a la Nota de MetaLink 293956.1 (login requerido) para mayor información en términos utilizados en la Actualización Crítica.

De acuerdo a Oracle, cuatro de las vulnerables corregidas en la Actualización Crítica de Oracle − Julio de 2006 afecta a las instalaciones para clientes de Base de Datos de Oracle.

Se cree que la vulnerabilidad en Oracle Database identificada como Oracle Vuln# DB06 en la Actualización Crítica de Oracle correspondiente a la Nota de Vulnerabilidad del US−CERT VU#932124, la cual incluye mayores detalles sobre soluciones temporales.

En la mayoría de los casos, Oracle no asocia identificadores Vuln# (por ejemplo DB01) con otra información disponible. Cuando lleguen a estar disponibles mayores detalles sobre vulnerabilidades y estrategias de solución serán actualizadas las notas de vulnerabilidades individuales.

III. Impacto

El impacto de éstas vulnerabilidades varía dependiendo del producto, componente y configuración del sistema. Las consecuencias potenciales incluyen la ejecución de código arbitrario o comandos, revelación de información y negación de servicio. Los componentes vulnerables podrían ser disponibles a intrusos remotos no autenticados. Un intruso que comprometa una base de datos de Oracle podría ser capaz de obtener acceso a información sensitiva.

IV. Solución

- **Aplicar una actualización de Oracle**

  Aplicar las actualizaciones apropiadas o actualizar la versión de acuerdo a lo especificado en la Actualización Crítica de Oracle −Julio de 2006. Se debe hacer notar que la Actualización Crítica solo lista los problemas corregidos recientemente. La actualizaciones para problemas anteriores no se encuentran listadas.

  Como se hizo notar en la actualización, algunas actualizaciones son acumulativas, otras no lo son:

  > *Las actualizaciones para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne and*

OneWorld Tools, y PeopleSoft Enterprise Portal Applications en las actualizaciones son acumulativas; cada una de las Actualizaciones Críticas contienen las soluciones de las Actualizaciones Críticas previas.

Las actualizaciones para Oracle E−Business Suite and Applications no son acumulativas, por lo que los usuarios de E−Business Suite and Applications deberían referirse a los Actualizaciones Críticas previas para identificar soluciones previas que desean aplicar.

Las actualizaciones de algunas plataformas y componentes no estuvieron disponibles cuando la Actualización Crítica fue publicada el 18 de Julio de 2006. Consulte la Nota de MetaLink 372930.1 (login requerido) para mayor información.

V. Apéndice A. Referencias

- Nota de Vulnerabilidad del US−CERT VU#932124 − <http://www.kb.cert.org/vuls/id/932124>
- Nota de Vulnerabilidad del US−CERTs Relacionada a la Actualización Crítica – Julio de 2006 − <http://www.kb.cert.org/vuls/byid?searchview&query=oracle_cpu_july_2006>
- Actualización Crítica – Julio de 2006 − <http://www.oracle.com/technology/deploy/security/pdf/cpujul2006.html>
- Actualizaciones Críticas y Alertas de Seguridad − <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Lista de Verificación de Seguridad para Oracle Database (PDF) − <http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf>
- Nota de MetaLink 293956.1 (login requerido) − <http://metalink.oracle.com/metalink/plsql/showdoc?db=Not&id=293956.1>
- Nota de MetaLink 372930.1 (login requerido) − <http://metalink.oracle.com/metalink/plsql/showdoc?db=Not&id=372930.1>
- Detalles sobre la Actualización Crítica de Oracle de Julio de 2006 − <http://www.red−database−security.com/advisory/oracle_cpu_jul_2006.html>

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

- Jesús Ramón Jiménez Rojas (jrojas 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